

service director processor generates for the ticket issuer a number that uniquely represents the user, establishes it as the customer number 9121, and registers that number in the customer table. The customer table is designated by using the customer table address 5230 of the ticket issuer list 5203.

[1579] Upon receiving the ticket order 5902, the ticket issuing system 107 decrypts it and examines the digital signature. The ticket issuing server 1100 updates the data in the customer information server 1101, the ticket issuing information server 1102 and the ticket information server 1103, generates ticket data (9219) for the ordered ticket, and transmits, to the service providing system, an electronic ticket issuing commission 5903, which constitutes a message requesting the process for issuing an electronic ticket that corresponds to the ticket and the process for settling the price of the ticket.

[1580] As is shown in Fig. 92A, the digital signature of a ticket issuer is provided for data that consists of an electronic ticket issuing commission header 9200, which is header information identifying the message as the electronic ticket issuing commission 5903 and describing the data structure; a transaction number 9201, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 9202, which conveys the price of a ticket; a clearing option 9203, which indicates which clearing procedures apply; a request number 9204; a ticket code 9205, which identifies the type of electronic ticket that is to be issued; a template code 9206, which identifies a template program to be used for an electronic ticket that is to be issued; a number of tickets 9207, which indicates how many tickets are to be issued; ticket data 9208; representative component information 9209; a ticket issuer ID 9210; and an issued time 9210, which is the date on which the electronic ticket issuing commission 5903 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket issuing commission 5903.

[1581] The clearing option 9203 is information by which the ticket issuing system designates, to the service providing system, the procedures to be used for clearing the price of a ticket. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic ticket to a user after the price of the ticket has been cleared, and a delayed clearing process for clearing the price of a ticket after an electronic ticket has been issued. The clearing option 9203 is used to designate either clearing process.

[1582] In the delayed clearing process, since an electronic ticket is issued to a user before the clearing process is performed, the user does not have to wait.

[1583] For example, based on a purchase history maintained for customers, the ticket issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known to be trustworthy, and can designate the spontaneous clearing for

a customer with whom it has had no previous dealings.

[1584] The ticket data 9208 is ticket information issued by the ticket issuer. A number of ticket information items equivalent to the number of tickets 9207 are established as the ticket data 9208. For one ticket, the digital signature of a ticket issuer is provided for data that consist of a ticket ID 9216, ticket information 9217 and a ticket issuer ID 9218, and the ticket information is thereby provided. The ticket information 9217 is ASCII information describing the contents of a ticket. For the ticket information 9217, the title of a ticket, the date, the location, the seat class, the sponsor and whether it can be transferred, and the usage condition information, such as the number of coupon tickets, when the ticket is used as a coupon ticket, are described using a form whereby tag information representing various information types is additionally provided.

[1585] The representative component information 9209 is information that is established as the representative component information 1932 for an electronic ticket to be generated. Therefore, the representative component information 9209 may not be set for use.

[1586] The ticket issuer processor of the service providing system receives the electronic ticket issuing commission 5903, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic ticket issuing process and the ticket price clearing process in accordance with the clearing procedures designated by using the clearing option 9203.

[1587] In Fig. 59 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1588] For the spontaneous clearing, the service director processor generates a clearing request 9324, which is a message requesting the clearing of the price of a ticket. The transaction processor processor closes the clearing request 9324 and addresses it to the transaction processor, and then transmits it as a clearing request 5904 to the transaction processing system 106.

[1589] As is shown in Fig. 93B, the digital signature of a service provider is provided for data that consists of a clearing request header 9314, which is header information indicating that the message is the clearing request 5904 and describing the data structure; a user clearing account 9315, which includes a credit card that corresponds to the payment service code designated by the user; a ticket issuer clearing account 9316, which designates the clearing account of a ticket issuer; a payment value 9317; a payment option code 9318; a request number 9319, which is issued by the mobile user terminal 100; a transaction number 9320, which is issued by the ticket issuing system; a validity term 9321, which presents the period during which the clearing request 5904 is effective; a service provider ID 9322; and an issued time 9323, which indicates the date on which the clearing request 5904 was issued. These data are closed and addressed to the transaction processor,

thereby providing the clearing request 5904.

[1590] The transaction processing system 106 receives the clearing request 5904, decrypts it and examines the digital signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 5905, and transmits it to the service providing system 110.

[1591] As is shown in Fig. 94A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 9400, which is header information indicating that the message is the clearing completion notification 5905 and describing the data structure; a clearing number 9401, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 9402; a ticket issuer clearing account 9403; a payment value 9404; a payment option code 9405; a request number 9406; a transaction number 9407; clearing information 9408 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 9409 for a ticket issuer that is accompanied by the digital signature of the transaction processor; clearing information 9410 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 9411; and an issued time 9412, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 5905.

[1592] Upon receiving the clearing completion notification 5905, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9413 to the service director processor. Upon receiving the clearing completion notification 9413, the service director processor generates a clearing completion notification 9430 for the ticket issuer. The ticket issuer processor closes the clearing completion notification 9430, and transmits it to the ticket issuing system 107 as a clearing completion notification 5906 for the ticket issuer.

[1593] As is shown in Fig. 94B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 9417, which is header information indicating that the message is the clearing completion notification 5906 and describing the data structure; a clearing number 9418; a customer number 9419; a ticket issuer ID 9420; a payment service code 9421; a payment value 9422; a payment option code 9423; a request number 9424; a transaction number 9425; clearing information 9426 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 9427; a service provider ID 9428; and an issued time 9429, which indicates the date on which the clearing completion notification was issued. These data are closed and

addressed to the ticket issuer, thereby providing the clearing completion notification 5906.

[1594] Upon receiving the clearing completion notification 5906, the ticket issuing system decrypts it and examines the digital signature, and generates a receipt 5907 and transmits it to the service providing system.

[1595] As is shown in Fig. 95A, the digital signature of a ticket issuer is provided for data that consists of a receipt header 9500, which is header information indicating that the message is the receipt 5907 and describing the data structure; a customer number 9501; ticket issuing information 9502; a payment service code 9503; a payment value 9504; a payment option code 9505; a request number 9506; a transaction number 9507; clearing information 9508; a transaction processor ID 9509; a ticket issuer ID 9510; and an issued time 9511, which indicates the date on which the receipt 5907 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 5907. The ticket issuing information 9502 is information concerning the ticket issuing process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1596] Upon receiving the receipt 5907, the ticket issuer processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 9512 to the service director processor. The service director processor employs the receipt 9512 to generate a receipt 9523 for a user.

[1597] In addition, the service director processor generates a clearing completion notification 9430 for the ticket issuing system, generates an electronic ticket to be issued to the user, and further generates an electronic ticket issuing message 9227 that includes the electronic ticket that is generated.

[1598] The user processor closes the electronic ticket issuing message 9227 and the receipt 9523 while addressing them to the user, and transmits them as an electronic ticket issuing message 5908 and a receipt 5909 to the mobile user terminal 100 via digital wireless communication.

[1599] As is shown in Fig. 92B, the digital signature of a service provider is provided for data that consist of an electronic ticket issuing header 9220, which is header information indicating that the message is the electronic ticket issuing message 5908 and describing the data structure; a transaction number 9221; a request number 9222; the number of tickets 9223; electronic ticket data 9224 that are generated; a service provider ID 9225; and an issued time 9226, which indicates the date on which the electronic ticket issuing message 5908 was issued. These data are closed and addressed to the user, thereby providing the electronic ticket issuing message 5908. The electronic ticket data 9224 includes electronic tickets 9231 equivalent in number to the number of tickets 9223.

[1600] As is shown in Fig. 95B, the digital signature of a service provider is provided for data that consists of a

receipt header 9516, which is header information indicating that the message is the receipt 5909 and describing the data structure; a user ID 9517; a receipt 9518 (9512) obtained by decryption; clearing information 9519 for a user that is accompanied by the digital signature of a transaction processor; ticket issuing information 9520; a service provider ID 9521; and an issued time 9522, which indicates the date on which the receipt 5909 was issued. These data are closed and addressed to the user, thereby providing the receipt 5909. The ticket issuing information 9520 is information for the electronic ticket issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1601] Upon receiving the electronic ticket issuing message 5908 and the receipt 5909, the mobile user terminal decrypts them and examines the digital signatures, enters in the ticket list 1712 an electronic ticket included in the electronic ticket issuing message 5908, enters the receipt 9523 in the use list 1715, and displays the electronic ticket on the LCD 303.

[1602] The generation of an electronic ticket by the service director processor is performed as follows.

[1603] First, the service director processor refers to the electronic ticket template list 4905 for the ticket issuer that is stored in the ticket issuer information server. Then, by using the electronic ticket template program that is identified by the template code 9206 of the electronic ticket issuing commission 5903, the service director processor generates a ticket program for an electronic ticket. Specifically, the ticket program data 1913 for an electronic ticket are generated using the transaction module and the display module, which are described as being located at the transaction module address 4919, and the display module address 4920 in the electronic ticket template list 4905, and the representative component information 9209 in the electronic ticket issuing commission 5903. When the representative component information 9209 is not present in the electronic ticket issuing commission 5903, the default representative component information located at the default representative component information address 4921 is employed as the information for an electronic ticket.

[1604] Following this and based on the usage condition information included in the ticket information 9217, the service director processor generates the ticket status 1907 and the variable ticket information 1908. Whether the ticket status 1907 can be transferred is designated, and when the ticket is used as a coupon ticket, the number of coupons is employed as the variable ticket information 1907. The service director processor generates a new pair consisting of a ticket signature private key and a ticket signature public key, and further generates the ticket program 1901 for an electronic ticket by employing the ticket private key and the gate public key that are registered in the electronic ticket management information 5300.

[1605] Furthermore, the service director processor generates an electronic ticket by employing the obtained ticket signature public key to generate the certificate 1903 for the electronic ticket, and by employing the ticket data 9219 in the electronic ticket issuing commission 5903 to generate the presentation ticket 1902 for the electronic ticket.

[1606] The procedures for the delayed clearing will now be described.

[1607] In Fig. 60 are shown the procedures for exchanging messages between the devices in the ticket purchase process for the delayed clearing. The same process is performed as is used for the spontaneous clearing until the ticket issuing system transmits the electronic ticket issuing commission to the service providing system.

[1608] When the delayed clearing is designated by the clearing option 9203, the service director processor generates an electronic ticket to be issued to the user, and also generates the electronic ticket issuing message 9227, which includes the generated electronic ticket, and a temporary receipt message 9310, which corresponds to a temporary receipt. The generation of the electronic ticket is performed in the same manner as that used for the spontaneous clearing.

[1609] The user processor closes the electronic ticket issuing message 9227 and the temporary receipt 9310 and addresses them to the user, and transmits these messages as an electronic ticket issuing message 6004 and a temporary receipt 6005 to the mobile user terminal 100 via digital wireless telephone communication.

[1610] As is shown in Fig. 93A, the digital signature of a service provider is provided for data that consists of a temporary receipt header 9300, which is header information indicating that the message is the temporary receipt 6005 and describing the data structure; a user ID 9301; ticket issuing information 9302; a payment service code 9303; a payment value 9304; a payment option code 9305; a request number 9306; a transaction number 9307; a service provider ID 9308; and an issued time 9309, which indicates the date on which the temporary receipt 6005 was issued. These data are closed and addressed to the user, thereby providing the temporary receipt 6005. The ticket issuing information 9302 is information concerning the electronic ticket issuing process that is performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1611] The data structure of the electronic ticket issuing message 6004 is the same as that used for the electronic ticket issuing message 5908.

[1612] Upon receiving the electronic ticket issuing message 6004 and the temporary receipt 6005, the mobile user terminal decrypts them and examines the digital signatures, enters an electronic ticket included in the electronic ticket issuing message 6004 in the ticket list 1712, enters the temporary receipt 9310 in the use list 1715, and displays the electronic ticket on the LCD

303.

[1613] Following this, the service director processor performs the clearing process for the price of the ticket. First, the service director processor generates a clearing request 9324, which is a message requesting the performance of the clearing process for the price of the ticket. The transaction processor closes the clearing request 9324 and addresses it to the transaction processor, and transmits it as a clearing request 6007 to the transaction processing system 106.

[1614] Upon receiving the clearing request 6007, the transaction processing system 106 decrypts it and examines the digital signature, and performs the clearing process. The transaction processing system 106 generates a clearing completion notification 6008 and transmits it to the service providing system 110.

[1615] Upon receiving the clearing completion notification 6008, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9413 to the service director processor. The service director processor employs the received clearing completion notification 9413 to generate a clearing completion notification 9430 for the ticket issuer. And the ticket issuer processor closes the clearing completion notification 9430 and transmits it to the ticket issuing system 107 as a clearing completion notification 6009 for the ticket issuer.

[1616] The ticket issuing system decrypts the received clearing completion notification 6009 and examines the digital signature, and generates a receipt 6010 and transmits it to the service providing system.

[1617] The ticket issuer processor of the service providing system decrypts the received receipt 6010 and examines the digital signature, and transmits a receipt 9512 to the service director processor. The service director processor employs the receipt 9512 to generate a receipt 9523 for a user.

[1618] The receipt 9523 that is generated is not immediately transmitted to the mobile user terminal 100 of the user. When the mobile user terminal has performed the data updating process, the user processor replaces the temporary receipt 9310 in the use list 1715 with the receipt 9523, and transmits the receipt 9523 as one part of the update data 6011 to the mobile user terminal 100.

[1619] The data structures of the clearing request 6007, the clearing completion notification 6008, the clearing completion notification 6009 and the receipt 6010 for the delayed clearing are the same as those provided for the clearing request 5904, the clearing completion notification 5905, the clearing completion notification 5906 and the receipt 5907 for the spontaneous clearing.

[1620] The delayed clearing process need not be performed immediately after the electronic ticket is issued, and together with the other clearing processes, may be performed, for example, once a day.

[1621] An explanation will now be given for the con-

tents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110 during the ticket registration processing.

[1622] In Fig. 65A are shown the procedures for exchanging messages between devices in the ticket registration processing, and in Figs. 106A and 106B are shown the contents of messages that are exchanged by the devices in the ticket registration processing.

[1623] First, when the user performs an electronic ticket registration operation 6500, the mobile user terminal generates a ticket registration request 6501 and transmits it to the service providing system via digital wireless telephone communication.

[1624] As is shown in Fig. 106A, the digital signature of a user is provided for data that consists of a ticket registration request header 10600, which is header information indicating that the message is the ticket registration request 6501 and describing the data structure; a ticket ID 10601 of a ticket to be registered; a user ID 10602; and an issued time 10603, which indicates the date on which the ticket registration request 6501 was issued. These data are closed and addressed to the service provider, thereby providing the ticket registration request 6501.

[1625] The user processor of the service providing system decrypts the received ticket registration request 6501 and examines the digital signature, and transmits the request 6501 to the service manager processor. The service manager processor generates a service director processor to form a process group that processes a ticket registration request 10604. The service director processor ascertains that the electronic ticket indicated by the ticket ID 10601 is registered in the ticket list 4610 for the user in the user information server 902, and registers that electronic ticket in the registered ticket list 5303 for electronic tickets of the service director information server 901. At this time, the service director processor newly generates a ticket signature private key and a ticket signature public key pair. Further, the service director processor generates a registered ticket certificate using the ticket signature public key, and registers it in the registered ticket list 5303. The service director processor then generates a ticket certificate issuing message 13313 using the ticket signature private key and the registered ticket certificate that has been generated. The user processor closes the ticket certificate issuing message 13313 and addresses it to the user, and transmits it as a ticket certificate issuing message 6502 to the mobile user terminal via digital wireless telephone communication.

[1626] As is shown in Fig. 106B, the digital signature of a service provider is provided for data that consists of a ticket certificate issuing header 10608, which is header information indicating that the message is the ticket certificate issuing message 6502 and describing the data structure; a ticket digital signature private key 10609; a registered ticket certificate 10610; a service provider ID 10611, and an issued time 10612, which

indicates the date on which the ticket certificate issuing message 6502 was issued. These data are closed and addressed to the user, thereby providing the ticket certificate issuing message 6502.

[1627] The mobile user terminal 100 decrypts the received ticket certificate issuing message 6502 and examines the digital signature, replaces the ticket signature private key and the ticket certificate of an electronic ticket with the ticket signature private key 10609 and the registered ticket certificate 10610, both of which are included in the ticket certificate issuing message 6502, changes the registration state in the ticket status to the post-registration state, and displays on the LCD the electronic ticket that has been registered (display a ticket that is registered; 6503).

[1628] An explanation will now be given for the contents of messages that are exchanged by the gate terminal 101 and the service providing system 110 during the ticket setup processing.

[1629] In Fig. 66 are shown procedures for exchanging messages between the devices in the ticket setup processing performed when the merchant sets up, at the gate terminal 101, a ticket to be examined. In Figs. 109A and 109B are the contents of messages that are exchanged by the devices during the ticket setup processing.

[1630] First, when the operator (merchant) of the gate terminal 101 performs a ticket setup operation 6600, the gate terminal generates a ticket setup request 6601 and transmits it to the service providing system via digital telephone communication.

[1631] As is shown in Fig. 109A, the digital signature of a merchant is provided for data that consists of a ticket setup request header 10900, which is header information indicating that the message is the ticket setup request 6601 and describing the data structure; a ticket code 10901 entered by the merchant during the ticket setup operation 6600; a gate ID 10902 for the gate terminal; a merchant ID 10903; and an issued time 10904, which indicates the date on which the ticket setup request 6601 was issued. These data are closed and addressed to the service provider, thereby providing the ticket setup request 6601.

[1632] The merchant processor of the service providing system decrypts the received ticket setup request 6601 and examines the digital signature, and transmits the request 6601 to the service manager processor. The service manager processor generates a service director processor to form a process group that processes a ticket setup request 10605. The service director processor ascertains that a merchant is registered in the merchant list 5302 for the electronic ticket that is identified by the ticket code 10901 for the service director information server 901. Then, the service director processor generates a ticket setup message 10919 by referring to the electronic ticket management information 5300, which is stored in the service director information server 901 for the pertinent electronic ticket, and

the electronic ticket template list 4905, which is stored in the ticket issuer information server 905 of the pertinent ticket issuer (the ticket issuer ID 5306). Specifically, the service director processor generates the ticket setup message 10919 by using the ticket examination module, which is located at the ticket examination module address 4922 in the electronic ticket template list 4905 that is identified by the template code 5312 of the electronic ticket management information 5300, and the ticket public key 5309 and the gate private key 5310, which are registered in the electronic ticket management information 5300. The merchant processor closes the ticket setup 10919 and addresses it to the merchant, and transmits it as a ticket setup message 6602 to the gate terminal via digital telephone communication.

[1633] As is shown in Fig. 109B, the digital signature of a service provider is provided for data that consists of a ticket setup header 10909, which is header information indicating that the message is the ticket setup message 6602 and describing the data structure; a ticket name 10910 for an electronic ticket to be issued; a ticket code 10911; a ticket issuer ID 10912; a validity term 10913; a gate private key 10914; a ticket public key 10915; a ticket examination module 10916; a service provider ID 10917; and an issued time 10918, which indicates the date on which the ticket setup message 6602 was issued. These data are closed and addressed to the merchant, thereby providing the ticket setup message 6602.

[1634] The mobile user terminal decrypts the received ticket setup message 6602 and examines the digital signature, registers, in the ticket list 2409, electronic ticket examination program information that is included in the ticket setup message 6602, and displays on the touch panel LCD a message indicating that the ticket setup process has been completed (display the setup completion; 6603).

[1635] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the gate terminal 101 during the ticket examination processing.

[1636] In Fig. 67 are shown procedures for the exchange of messages by the devices during the ticket examination processing, and in Figs. 110A and 110B and Figs. 111A and 111B are the contents of the messages that are exchanged by the devices during the ticket examination processing.

[1637] First, when a user performs a ticket presentation operation 6700, the mobile user terminal generates a ticket presentation message 6701 by using an electronic ticket to be examined and an arbitrarily generated test pattern, and transmits it to the gate terminal via infrared communication.

[1638] As is shown in Fig. 110A, the ticket presentation message 6701 consists of a ticket presentation header 11000, which is header information indicating that the message is the ticket presentation message 6701 and describing the data structure; a service code

11001, which identifies the request for the examination of an electronic ticket; a request number 11002, which is an arbitrarily generated number that uniquely represents the ticket examination process; a ticket 11003 for presenting an electronic ticket to be examined; a ticket certificate 11004; the current ticket status of an electronic ticket that is to be examined; variable ticket information 11006; a ticket ID 11007; an issued time 11008, which indicates the date on which the ticket presentation message 6701 was issued; and a gate test pattern 11010, which is an arbitrarily generated test pattern. The digital signature is provided, using the ticket signature private key of an electronic ticket, for the ticket status 11005, the variable ticket information 11006, the ticket ID 11007 and the issued time 11008. The gate test pattern is encrypted using the gate public key.

[1639] The presentation ticket 11003, the ticket certificate 11004, the ticket status 11005, the variable ticket information 11006, the ticket ID 11007 and the issued date 11008 specify the contents of the electronic ticket for the gate terminal, and the gate test pattern 11010 is a test pattern for authorizing the gate terminal.

[1640] Upon receiving the ticket presentation message 6701, first, the gate terminal refers to the ticket list 2409, activates a ticket examination module that corresponds to the ticket code of the electronic ticket that is presentation, examines the validity of the contents of the ticket presentation message 6701, and generates a ticket examination message 6702 and transmits it to the mobile user terminal via infrared communication.

[1641] In the verification process for the validity of the ticket presentation message 6701, the gate terminal employs the fact that the ticket certificate 11004 is a registered ticket certificate and examines the ticket status 11005 and the variable ticket information 11006 to determine whether an electronic ticket that is to be examined is valid. Then, the gate terminal examines the presentation ticket 11003, the digital signature of the service provider that is provided for the ticket certificate 11004, and the validity term. Further, the gate terminal employs the ticket signature public key of the ticket certificate 11004 to examine the digital signature of the electronic ticket that is provided for the ticket status 11005, the variable ticket information 11006, the ticket ID 11007, and the issued time 11008. Thus, the validity of the ticket presentation message 6701 is verified.

[1642] In the generation of the ticket examination message 6702, the gate terminal decrypts the gate test pattern 11010 using the gate private key, and employs the ticket public key to encrypt the ticket test pattern 11108 that is arbitrarily generated.

[1643] As is shown in Fig. 110B, the digital signature of a merchant is provided for the data that consists of a ticket examination header 11012, which is header information indicating that the message is the ticket examination message 6702 and describing the data structure; a transaction number 11013; a response message 11014; a request number 11015; a ticket ID 11016; an

instruction code 11017; a gate test pattern 11018, which is decrypted; a ticket test pattern 11019, which is an arbitrarily generated test pattern; a gate ID 11021; a merchant ID 11022; and an issued time 11023, which indicates the date on which the ticket examination message 6702 was issued. Thus, the ticket examination 6702 is provided. The ticket test pattern 11019 is encrypted using the ticket public key.

[1644] The transaction number 11013 is a number, arbitrarily generated by the gate terminal, that uniquely represents the ticket examination process. When, as a result of the examination of the ticket presentation message 6701, the ticket examination process can not be performed (the electronic ticket is one that can not be examined by the pertinent gate terminal), a value of 0 is set. When the ticket examination process can be performed, a value other than 0 is set.

[1645] The response message 11014 is text information constituting the message transmitted by the merchant to the user. When the gate terminal can not examine an electronic ticket that is presented (transaction number = 0), data to that effect is included in the response message. The response message is optionally set, and may not be reset.

[1646] The instruction code 11017 is command code information for an electronic ticket that indicates how the ticket status and variable ticket information of the electronic ticket can be changed. The instruction code is varied by combining the electronic ticket transaction module and the ticket examination module.

[1647] When the mobile user terminal receives the ticket examination message 6702, first, in order to verify the gate terminal the mobile user terminal compares the gate test pattern 11010 with the gate test pattern 11018 included in the ticket examination message 6702, and changes the ticket status and the variable ticket information of the electronic ticket in accordance with the instruction code 11017. Then, the mobile user terminal decrypts the ticket test pattern using the ticket private key, generates a ticket examination response 6703, and transmits it to the gate terminal via infrared communication.

[1648] As is shown in Fig. 111A, the digital signature using the ticket signature private key and the digital signature of a user are provided for the data that consist of a ticket examination response header 11100, which is header information indicating that the message is the ticket examination response 6703 and describing the data structure; a ticket examination number 11101, which indicates the order of the ticket examination process; a ticket test pattern 11102, which is decrypted; a ticket status 11103 and variable ticket information 11104, which are modified; a gate ID 11105; a merchant ID 11106; a request number 11107; a transaction number 11108; a ticket code 11109; a ticket ID 11110; and an issued time 11111, which indicates the date on which the ticket examination response 6703 was issued. In this fashion, the ticket examination response

6703 is provided.

[1649] Upon receiving the ticket examination response 6703, first, the gate terminal authorizes the electronic ticket by comparing the ticket test pattern 111019 with the ticket test pattern 11102 that is included in the ticket examination response 6703, examines the validity of the contents of the ticket examination response 6703, and generates an examination certificate 6704 and transmits it to the mobile user terminal via infrared communication.

[1650] In the verification process for the validity of the ticket examination response 6703, the gate terminal determines whether the ticket status 11103 and the variable ticket information 11104 have been changed in accordance with the instruction code 11107, and examines the digital signature of the ticket examination response 6703.

[1651] As is shown in Fig. 111B, the digital signature of a merchant is provided for the data that consist of an examination certificate header 11113, which is header information indicating that the message is the examination certificate 6704 and describing the data structure; examination information 11114, which is text information indicating the contents of the ticket examination process; a ticket ID 11115; a request number 11116; a transaction number 11117; a ticket examination number 111187; a gate ID 11119; a merchant ID 11120; and an issued time 11121, which indicates the date on which the examination certificate 6704 was issued. In this fashion, the examination certificate 6704 is provided.

[1652] Upon receiving the examination certificate 6704, the mobile user terminal increments the ticket examination number, registers the examination certificate 6704 as usage information in the use list 1715, and displays the examined electronic ticket on the LCD (display the examined ticket; 6706).

[1653] When the gate terminal has transmitted the examination certificate 6704, the gate terminal registers, in the transaction list 2510, the ticket examination response 6703 as history information for the ticket examination process, and displays the results obtained during the ticket examination process on the touch panel LCD (display the results of examination; 6705). When the gate opening/closing device is connected to the gate terminal, the gate is automatically opened (entrance permission 6707).

[1654] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket reference processing.

[1655] In Fig. 71 are shown procedures for the exchange of messages by the devices during the ticket reference processing, and in Figs. 88A to 88D and Fig. 116A are shown the contents of messages that are exchanged during the ticket reference processing.

[1656] The ticket reference processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates

the data in the gate terminal.

[1657] Therefore, for the ticket reference process, the procedures for the exchange of messages by the gate terminal and the service providing system, and the contents (data structures) of the messages to be exchanged are the same as those employed for the above described data updating processing.

[1658] Compressed upload data 8818 in the upload data 5702 include a ticket examination response that is newly registered in the transaction list 2510 during the ticket examination process conducted during the period extending from the previous performance of the data updating process to the current performance of the data updating process.

[1659] During the data updating processing, the merchant processor transmits, to the service manager processor, a message requesting the reference process be performed for the ticket examination response that is uploaded from the gate terminal. The service manager processor generates a service director processor to form a process group for examining the validity of the ticket examination response.

[1660] First, the service director processor determines whether the gate ID 11105 and the merchant ID 11106 in the ticket examination response match the gate ID 5215 of the merchant and the merchant ID 5214. Then, the service director processor examines the registered ticket list 5303 in the service director information server 901 to verify that the electronic ticket for which the ticket examination response was issued is registered. The service director processor employs the user public key 5323 to examine the digital signature of the user that accompanies the ticket examination response, and employs the registered ticket certificate to examine the digital signature for the ticket that accompanies the ticket examination response. In addition, the service director processor employs the ticket examination number when examining the matching of the ticket status with the variable ticket information that has been modified, and transmits the result of the examination to the merchant processor. As a result, the ticket examination response is registered in the ticket examination response list.

[1661] The merchant processor enters the received ticket reference results in the compressed update data 8828 in the update data 5705, and transmits the data 5705 to the gate terminal.

[1662] When an error occurs in the process for verifying the validity of the ticket examination response, the service director processor transmits a message indicating that an error occurred in the management system 908.

[1663] Upon receiving the update data 5705, the gate terminal decompresses the update data 8828 and updates the data in the RAM and on the hard disk. At this time, the ticket reference results are registered in the authorization report list 2511 of the gate terminal.

[1664] If the firm represented by the merchant differs

from that represented by the ticket issuer and a payment is made by the ticket issuer to the merchant who handles the ticket, or if the usage of the ticket is periodically reported to the ticket issuer in accordance with the terms of a contract, in accordance with the ticket examination response that is newly registered in the ticket examination response list, the service director processor generates weekly, for example, a usage condition notification 11606, which is a message for notifying the ticket issuer of the ticket usage condition. The ticket issuer processor closes the notification 11606 and addresses it to the ticket issuer, and transmits it as a usage report 7100 to the ticket issuing system 107.

[1665] As is shown in Fig. 116A, the digital signature of a service provider is provided for the data that consists of a usage report header 11600, which is header information indicating that the message is the usage report 7100 and describing the data structure; a ticket ID list 11601 of tickets that are employed; the merchant name 11602 and the merchant ID 11603 of a merchant that handles the ticket; a service provider ID 11604; and an issued time 11605, which indicates the date on which the usage report 7100 was issued. These data are closed and addressed to the ticket issuer, thereby providing the usage report 7100.

[1666] Upon receiving the usage report 7100, the ticket issuing system 107 decrypts it and examines the digital signature, and performs such processing as making a payment to the merchant.

[1667] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket transfer processing.

[1668] In Fig. 74 are shown procedures for the exchange of messages by the devices during the ticket transfer processing, and in Figs. 117A and 117B, 118A and 118B, and 119A and 119B are shown the contents of messages that are exchanged during the ticket transfer processing. The ticket transfer process can be performed when the ticket status 1907 of the electronic ticket indicates the transfer enabled state, which is designated by the ticket issuer when issuing a ticket.

[1669] In Fig. 74 is shown a case where user A transfers an electronic ticket to user B. The procedures for the exchange of messages by the devices belonging to users A and B are the same for infrared communication as they are for digital wireless communication. The data structures of messages are also the same.

[1670] In Fig. 74, first, when user A performs a ticket transfer process 7400, the mobile user terminal of user A transmits a ticket transfer offer 7401, which is a message offering to transfer an electronic ticket, to the mobile user terminal of user B. When at this time the mobile user terminals of user A and user B are connected, communication between user A and user B is performed via digital wireless telephone. When the mobile user terminals are not connected, infrared communication is employed.

[1671] As is shown in Fig. 117A, the digital signature

of user A is provided for the data consisting of a ticket transfer offer header 11700, which is header information indicating that the message is the ticket transfer offer 7401 and describing the data structure; a transfer offer number 11701, which is an arbitrarily generated number that uniquely represents the ticket transfer process; a presentation ticket 11702 and a ticket certificate 11703 for an electronic ticket to be transferred; a ticket status 11704; variable ticket information 11705; a ticket ID 11706; an issued time 11707, which indicates the date on which the ticket transfer offer 7401 was issued; and a user public key certificate 11709. In this fashion, the ticket transfer offer 7401 is provided. The digital signature of the electronic ticket is provided, using the ticket signature private key, for the ticket status 11704, the variable ticket information 11705, the ticket ID 11706 and the issued time 11707.

[1672] The digital signature of the service provider is provided for the data that consist of a user public key header 11710; the user public key 11711 of user A; a public key certificate ID 11712, which is ID information for the public key certificate; a certificate validity term 11713; a service provider ID 11714; and a certificate issued time 11715. In this fashion, the user public key certificate 11709 is provided.

[1673] Upon receiving the ticket transfer offer 7401, the mobile user terminal of user B examines the presentation ticket 11702, the ticket certified 11703, and the digital signature of the service provider and the validity term of the public key certificate 11709. Then, the mobile user terminal examines the digital signature of the electronic ticket that is provided for the ticket status 11704, the variable ticket information 11705, the ticket ID 11706 and the issued time 11707, and the digital signature of user A accompanying the ticket transfer offer 7401, and verifies the contents of the ticket transfer offer 7401. In accordance with the presentation ticket 11702, the ticket status 11704 and the variable ticket information 11705, the mobile user terminal then displays, on the LCD, the contents of the electronic ticket that is to be transferred (display the transfer offer; 7402).

[1674] When user B performs a transfer offer acceptance operation 7403, the mobile user terminal of user B transmits, to the mobile user terminal of user A, a ticket transfer offer response 7404, which is a response message for the ticket transfer offer 7401.

[1675] As is shown in Fig. 117B, the digital signature of user B is provided for the data that consist of a ticket transfer offer response header 11716, which is header information indicating that the message is the ticket transfer offer response 7404 and describing the data structure; an acceptance number 11717; a transfer offer number 11718; a ticket ID 11719; an issued time 11720, which indicates the date on which the ticket transfer offer response 7404 was issued; and a user public key certificate 11721. In this fashion, the ticket transfer offer response 7404 is provided.

[1676] The user public key certificate 11721 is a public

key certificate for user B. To provide this certificate 11721, the digital signature of the service provider is provided for the data that consist of a user public key certificate header 11722; a user public key 11723 for user B; a public key certificate ID 11724, which is ID information for the public key certificate; a certificate validity term 11725; a service provider ID 11726; and a certificate issued time 11727.

[1677] The acceptance number 11717 is arbitrarily generated, by the mobile user terminal of user B, as a number that uniquely represents the ticket transfer processing. With this number, the mobile user terminal of user A is notified as to whether user B has accepted the ticket transfer offer 7401. When user B does not accept the ticket transfer offer 7401, a value of 0 is set as the acceptance number 11717. When user B accepts the ticket transfer offer 7401, a value other than 0 is set.

[1678] Upon receiving the ticket transfer offer response 7404, the mobile user terminal of user A displays, on the LCD, the contents of the ticket transfer offer response 7404 (display the transfer offer response; 7405). When the ticket transfer offer 7401 is accepted (acceptance number 11717 \neq 0), the mobile user terminal of user A examines the digital signature of the service provider of the user public key certificate 11721 and the validity term. The mobile user terminal generates a ticket transfer certificate 7406, which is a message that corresponds to a transfer certificate for an electronic ticket to user B, and transmits it to the mobile user terminal of user B.

[1679] As is shown in Fig. 118A, the digital signature of the electronic ticket and the digital signature of user A are provided for the data that consist of a ticket transfer certificate header 11800, which is header information indicating that the message is the ticket transfer certificate 7406 and describing the data structure; a presentation ticket 11801 for an electronic ticket to be transferred; a ticket status 11802; variable ticket information 11803; a transfer offer number 11804; an acceptance number 11805; a public key certificate ID 11806 for the user public key certificate of user B; a public key certificate ID 11807 for the user public key certificate of user A; a ticket ID 11808; and an issued time 11809, which indicates the date on which the ticket transfer certificate 7406 was issued. These data are closed and addressed to user B, thereby providing the ticket transfer certificate 7406.

[1680] Upon receiving the ticket transfer certificate 7406, the mobile user terminal of user B decrypts it and examines the digital signature of user A and the one accompanying the electronic ticket. Further, the mobile user terminal compares the ticket ID presented by the ticket transfer offer 7401 with the ticket ID 11808, and compares the public key certificate IDs 11806 and 11807 with the public key certificates of users B and A to verify the contents of the ticket transfer certificate 7406. The mobile user terminal then generates a ticket

transfer receipt 7407, which is a message indicating the electronic ticket has been received, and transmits the receipt 7407 to the mobile user terminal of user A.

[1681] As is shown in Fig. 118B, the digital signature of user B is provided for the data that consist of a ticket transfer receipt header 11815, which is header information indicating that the message is the ticket transfer receipt 7407 and describing the data structure; a ticket ID 11816; a transfer offer number 11817; an acceptance number 11818; a public key certificate ID 11819 for the user public key certificate of user A; a public key certificate ID 11820 for the user public key certificate of user B; and an issued time 11821, which indicates the date on which the ticket transfer receipt 7407 was issued. These data are closed and addressed to user A, thereby providing the ticket transfer receipt 7407.

[1682] Upon receiving the ticket transfer receipt 7407, the mobile user terminal of user A decrypts it, and examines the digital signature of user B. Further, the mobile user terminal compares the public key certificate IDs 11819 and 11820 with the public key certificates of users B and A to verify the contents of the ticket transfer receipt 7407. The mobile user terminal then erases the transferred electronic ticket from the ticket list 1712, and registers the ticket transfer receipt 11822 in use history 1715. At this time, addresses in the object data area at which the transfer offer number, the code information indicating the ticket transfer process, the issued time for the ticket transfer receipt 7407 and the ticket transfer receipt 11822 are stored are assigned to the request number 1840 in the use list 1715, the service code 1841, the use time 1842 and the use information address 1843.

[1683] The mobile user terminal of user A displays, on the LCD, a message indicating the completion of the transfer process (display the transfer process; 7408). The process at the mobile user terminal of user A (sender) is thereafter terminated.

[1684] After transmitting the ticket transfer receipt 7407, the mobile user terminal of user B displays the received ticket transfer certificate 11811 on the LCD. In addition, the mobile user terminal displays a dialogue message inquiring whether the transfer process with the service providing server (process for downloading the received electronic ticket from the service providing system) should be immediately performed (display the transfer certificate; 7409).

[1685] The dialogue message has two operating menus: "transfer process request" and "cancel." When "cancel" is selected, the transfer process performed with the service providing server is canceled, and in the process (data updating process) during which the service providing system updates the data in the mobile user terminal, an electronic ticket that has been transferred is assigned to the mobile user terminal.

[1686] When user B selects "transfer process request" (transfer process request operation; 7410), based on the ticket transfer certificate 11811 the mobile user ter-

minal generates a ticket transfer request 7411, which is a message requesting that the transfer process be performed with the service providing system, and transmits it to the service providing system via digital wireless telephone communication.

[1687] As is shown in Fig. 119A, the digital signature of user B is provided for the data that consists of a ticket transfer request header 11900, which is header information indicating that the message is the ticket transfer request 7411 and describing the data structure, a decrypted ticket transfer certificate 11901 (11811); the user ID 11902 of user B; and an issued time 11903, which indicates the date when the ticket transfer request 7411 was issued. These data are closed and addressed to the service provider, thereby providing the ticket transfer request 7411.

[1688] Upon receiving the ticket transfer request 7411, the user processor of user B of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the ticket transfer request 11904.

[1689] The service director processor, first refers to the user list 5200 and specifies the recipient (user B) and the sender (user A) of the transfer process by employing the public key certificate IDs 11806 and 11807 in the ticket transfer certificate 11901 that is included in the ticket transfer request 11904. The service director processor examines the digital signature of the user A and the digital signature accompanying the electronic ticket, which are provided for the ticket transfer certificate 11901, and verifies the validity of the ticket transfer certificate 11901. Following this, the service director processor exchanges the user ID 5317 for the user A with that for the user B in the user list 5301 for the electronic ticket that is stored in the service director information server 901, and erases the electronic ticket to be transferred from the ticket list of the user A that is stored in the user information server 902. Then, the service director processor changes the ticket signature private key and ticket signature public key pair and the ticket certificate for a new key pair and a ticket certificate, and also changes the ticket status and the variable ticket information to the ticket status 11802 and to the variable ticket information 11803 for the ticket transfer certificate 11901. The service director processor generates an electronic ticket received from user A, and enters it in the ticket list 4610 for the user B.

[1690] When the electronic ticket that is to be transferred has already been registered, the service director processor updates the registered ticket list 5303 holding the electronic ticket. Specifically, the user ID 5322, the user public key 5323, the registered ticket certificate address 5324, the ticket examination response list address 5325 and the former user information address 5326, all of which are in the registered ticket list 5303, are updated (to the information for user B). The old

information (information for user A) is pointed to at the former user information address 5326 as former user information 5327.

[1691] The service director processor generates a ticket transfer message 11915, which includes an electronic ticket transferred from user A. The user processor of user B closes the message 11915 and addresses it to the user B, and transmits it as a ticket transfer message 7412 to the mobile user terminal of user B via digital wireless telephone communication.

[1692] As is shown in Fig. 119B, the digital signature of the service provider is provided for the data that consist of a ticket transfer header 11908, which is header information indicating that the message is the ticket transfer 7412 and describing the data structure; a transfer number 11909, which is an arbitrarily generated number that represents the transfer process in the service providing system; transfer information 11910; an acceptance number 11911; an electronic ticket 11912, which is transferred; a service provider ID 11913; and an issued time 11914, which indicates the date when the ticket transfer message 7412 was issued. These data are closed and addressed to the user B, thereby providing the ticket transfer message 7412.

[1693] The transfer information 11910 is information concerning the electronic ticket transfer process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1694] The mobile user terminal of user B decrypts the received ticket transfer message 7412 and examines the digital signature, registers the electronic ticket 11912 in the ticket list 1712, and displays the electronic ticket on the LCD (display the electronic ticket; 7413). The ticket transfer process is thereafter terminated.

[1695] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket installation processing.

[1696] In Fig. 77 are shown procedures for the exchange of messages by the devices during the ticket installation processing, and in Figs. 123A and 123B, and 124A and 124B are shown the contents of messages that are exchanged during the ticket installation processing.

[1697] First, when the user performs an electronic ticket installation operation 7700, the mobile user terminal generates an electronic ticket installation request 7701, and transmits it to the service providing system 110 via digital wireless telephone communication.

[1698] As is shown in Fig. 123A, the digital signature of the user is provided for the data that consists of an electronic ticket installation request header 12300, which is header information indicating that the message is the electronic ticket installation request 7701 and describes the data structure; an installation card number 12301 and an installation number 12302, which are entered by a user; a request number 12303, which is an arbitrarily generated number that uniquely represents the electronic ticket installation process; a user ID

12304; and an issued time 12305, which indicates the date when the electronic ticket installation request 7701 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket installation request 7701.

[1699] Upon receiving the electronic ticket installation request 7701, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the electronic ticket installation request 12306.

[1700] First, the service director processor refers to the installation card list that is indicated by the installation card list address 5229 for the ticket issuer list 5203, and specifies a ticket issuer who issues a ticket that is represented by the installation number 12301. The service director processor generates a ticket installation request 12317, which is a message requesting that the ticket issuer issue a ticket using the installation card. The ticket issuer processor closes the request 12317 and addresses it to the ticket issuer, and transmits it as a ticket installation request 7702 to the ticket issuing system 107.

[1701] As is shown in Fig. 123B, the digital signature of the service provider is provided for the data that consist of a ticket installation request header 12310, which is header information indicating that the message is the ticket installation request 7702 and describing the data structure; an installation card number 12311; an installation number 12312; a request number 12313; a customer number 12314, which uniquely represents a user for the ticket issuer; a service provider ID 12315; and an issued time 12316, which indicates the date when the ticket installation request 7702 was issued. These data are closed and addressed to the ticket issuer, thereby providing the ticket installation request 7702.

[1702] Upon receiving the ticket installation request 7702, the ticket issuing system 107 decrypts it and examines the digital signature. The ticket issuing server 1100 compares the installation card number 12311 and the installation number 12312, which are included in the ticket installation request 7702, with the management information for the issued electronic ticket installation card that is stored in the ticket issuing information server 1102. The ticket issuing server 1100 then updates the data in the customer information server 1102 and the ticket issuing information server 1103. Furthermore, the ticket issuing server generates ticket data (12406) for a requested ticket, and transmits, to the service providing system, an electronic ticket installation commission 7703, which is a message requesting the installation of an electronic ticket that corresponds to the requested ticket.

[1703] As is shown in Fig. 124A, the digital signature of the ticket issuer is provided for the data that consists of an electronic ticket installation commission header

12400, which is header information indicating that the message is the electronic ticket installation commission 7703 and describing the data structure; a transaction number 12401, which is an arbitrarily generated number that uniquely represents the transaction with a user; ticket issuing information 12402; a request number 12403; ticket code 12404, which indicates the type of electronic ticket that is to be issued; a template code 12405, which indicates a template program for an electronic ticket to be issued; ticket data 12406; representative component information 12407; a ticket issuer ID 12408; and an issued time 12409, which indicates the date when the electronic ticket installation commission 7703 was issued. These data are closed and addressed to the service provider, thereby providing the electronic ticket installation commission 7703.

[1704] The ticket issuing information 12402 is information concerning the ticket issuing process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1705] The ticket data 12406 is ticket information issued by the ticket issuer, wherein the digital signature of the ticket issuer accompanies the data that consists of the ticket ID 12414, the ticket information 12415 and the ticket ID 12416.

[1706] The ticket issuer processor of the service providing system decrypts the received electronic ticket installation commission 7703 and examines the digital signature, and transmits the commission 7703 to the service director processor. In accordance with the electronic ticket installation commission 12410, the service director processor generates an electronic ticket to be issued to a user, using the same procedures as are used for the ticket purchase processing, and also generates an electronic ticket installation message 12415, which is a message directing that the electronic ticket be installed in the mobile user terminal. The user processor closes the electronic ticket installation message 12455 and addressees it to a user, and transmits it as an electronic ticket installation message 7704 to the mobile user terminal via digital wireless telephone communication.

[1707] As is shown in Fig. 124B, the digital signature of the service provider is provided for the data that consists of an electronic ticket installation header 12417, which is header information indicating that the message is the electronic ticket installation message 7704 and describing the data structure; a transaction number 12418; ticket issuing information 12419, which concerns the ticket issuing process performed by the ticket issuing system; ticket issuing information 12420, which concerns the ticket issuing process performed by the service providing system; a request number 12421; generated electronic ticket code 12422; a service provider ID 12423; and an issued time 12424, which indicates the date when the electronic ticket installation message 7704 was issued. These data are closed and addressed to the user, thereby providing the electronic

ticket installation message 7704. The ticket issuing information 12419 and the ticket issuing information 12420 are accompanied by the digital signatures of the ticket issuer and the service provider.

[1708] The mobile user terminal decrypts the received electronic ticket installation message 7704 and examines the digital signature, registers, in the ticket list 1712, the electronic ticket included in the electronic ticket installation request 7704, and displays the installed electronic ticket on the LCD (display the electronic ticket; 7705).

[1709] An explanation will now be given for the contents of messages that are exchanged by the devices during the ticket modification processing.

[1710] In Fig. 80 are shown procedures for the exchange of messages by the gate terminal 101, the service providing system 110 and the ticket issuing system 107 during the processing performed to modify the ticket examination program of the gate terminal. In Figs. 129A and Figs. 88C, 88D and 88F are shown the contents of messages that are exchanged by the gate terminal 101, the service providing system 110 and the ticket issuing system 107 during the ticket modification processing. In Fig. 81 are shown procedures for the exchange of messages by the mobile user terminal 100, the service providing system 110 and the ticket issuing system 107 during the processing performed to modify the electronic ticket of the mobile user terminal. In Figs. 129A and 129B, and Figs. 130A and 130B are shown the contents of messages that are exchanged by the mobile user terminal 100, the service providing system 110 and the ticket issuing system 107.

[1711] When the contents of a ticket that was issued must be altered because an event was changed or an error was found when the ticket was issued, the ticket issuing system generates a modification request 8000 or 8100, which is a message requesting the modification of a ticket that was issued, and transmits it to the service providing system.

[1712] As is shown in Fig. 129A, the digital signature of the ticket issuer is provided for the data that consist of a modification request header 12900, which is header information indicating that the message is the modification request 8000 or 8100 and describing the data structure; a modification number 12901, which is an arbitrarily generated number that uniquely represents the ticket modification processing; a modification code 12902; a modification time limit 12903, which indicates the time limit for the modification; a modification message 12904; a ticket code 12905, which indicates the type of electronic ticket that is to be modified; a template code 12906, which identifies a template program for a modified electronic ticket; a ticket count 12907 that indicates the number of electronic tickets to be modified; modified ticket data 12908; modified representative component information 12909; a ticket issuer ID 12910; and an issued time 12911, which indicates the date when the ticket modification request 8000 was issued.

These data are closed and addressed to the service provider, thereby providing the ticket modification request 8000 or 8100.

[1713] The modification code 12902 is code information that identifies the type of ticket modification processing, and that indicates the modification of the electronic ticket information 1917, the modification of the representative component information 1932, the modification of the template program, or the modification accompanied by the ticket refund processing will be performed.

[1714] The modification message 12904 specifies the contents of the modification, and is accompanied by the digital signature of the ticket issuer.

[1715] The ticket data 12908 is modified ticket information for an electronic ticket to be modified. Tickets in a number equivalent to the ticket count 12907 are set as ticket data 12908. The ticket information is obtained by providing the digital signature of the ticket issuer for the data that consists of the ticket ID 12916, the ticket information 12917 and the ticket issuer ID 12918. When no modification of the electronic ticket information is to take place, the ticket data 12908 are not set.

[1716] The representative component information 10209 is set as the modified representative component information 1932 for an electronic ticket that is to be modified. When no modification is scheduled for the representative component information 1932, the representative component information 10209 is not set.

[1717] The ticket issuer processor of the service providing system 110 decrypts the received modification request 8000 or 8100 and examines the digital signature, and transmits the request to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the modification request 12912. Then, the service director processor changes the electronic ticket of the mobile user terminal and the ticket examination program of the gate terminal in accordance with the modification request 12912. The ticket examination program for the gate terminal is changed when the template program is modified.

[1718] An explanation will now be given for the processing performed to change the ticket examination program for the gate terminal.

[1719] First, the service director processor generates a new ticket examination program by employing the ticket examination module, which is pointed to at the ticket examination module address 4922 in the electronic ticket template list 4905 indicated by the template code 12906, and the ticket public key 5309 and the gate private key 5310, which are registered in the electronic ticket management information 5300. Then, the service director processor refers to the examination ticket list 4711 for the gate terminal of the merchant who is registered in the merchant list 5302 to obtain the electronic ticket that is to be modified, and specifies that the gate terminal for which the electronic ticket to be modified is

registered is an electronic ticket that the gate terminal is to examine. The service director processor transmits, to the merchant processor of the gate terminal that is specified, a message requesting the performance of the forcible data updating process to update the ticket examination program.

[1720] The merchant processor of the specified gate terminal performs the forcible data updating process, and modifies the ticket examination program of the gate terminal. At this time, the procedures for the exchange of messages by the gate terminal and the service providing system, and the contents (data structures) of the messages that are exchanged are the same as those employed for the forcible data updating processing that was previously described.

[1721] The merchant processor inserts the new ticket examination program into the compressed update data 8828 of the update data 5708, and transmits the resultant data to the gate terminal as the update data 5708.

[1722] Upon receiving the update data 5708, the gate terminal decompresses the update data 8828, and updates the data in the RAM and on the hard disk. At this time, the ticket examination program is also registered in the ticket list 2409 of the gate terminal.

[1723] An explanation will now be given for the processing for modifying an electronic ticket in the mobile user terminal. First, the service director processor refers to the user list 5301 for an electronic ticket to be modified, and specifies a user who owns the electronic ticket that is to be modified. The service director processor generates a modification notification 12928, which is a message for notifying the specified user of the modification of the electronic ticket. The user processor for the specified user closes the modification notification 12928, addresses it to the user, and transmits it as a modification notification 8101 to the mobile user terminal via digital wireless telephone communication.

[1724] As is shown in Fig. 129B, the digital signature of the service provider is provided for the data that consist of a modification notification header 12920, which is header information indicating that the message is the modification notice 8101 and describing the data structure; a modification number 12921; a modification code 12922; a ticket ID 12923; a modification message 12924; a reply time limit 12925, which specifies the time limit for the transmission of a replay (reaction selection 8104) by the user to the modification notice 8101; a service provider ID 12926; and an issued time 12927, which indicates the date on which the modification notice 8101 was issued. These data are closed and addressed to the user, thereby providing the modification notice 8101.

[1725] Upon receiving the modification notice 8101, the mobile user terminal decrypts it and examines the digital signature, outputs a call arrival tone to notify the user of the reception of the modification notice 8101, and displays a modification message 12924 on the LCD (display the modification notice; 8102). For example,

when the date has been changed, a message to that effect and a message requesting that the user select an action, either "accept," "refuse" or "refund," in response to the modification are displayed.

[1726] When, in response to the message displayed on the LCD, the user employs the number key switches to select an action in response to the modification (reaction selection operation 8103), the mobile user terminal generates a reaction selection message 8104, which contains the response of the user to the modification notice 8101, and transmits it to the service providing system via the digital wireless telephone communication. When the user selects "refuse" or "refund," the mobile user terminal changes the ticket status 1907 of the electronic ticket to the use disabled state.

[1727] As is shown in Fig. 130B, the digital signature of the user is provided for the data that consists of a reaction selection header 13000, which is header information indicating that the message is the reaction selection message 8104 and describing the data structure; a modification number 13001; a reaction code 13002, which identifies the type of reaction to the modification that the user selected; a ticket ID 13004, which is a number that is arbitrarily generated, by the mobile user terminal, that uniquely represents the ticket modification; a user ID 13005; and an issued time 13006, which indicates the date on which the selection message 8104 was issued. These data are closed and addressed to the service provider, thereby providing the reaction selection message 8104.

[1728] The user processor of the service providing system decrypts the received reaction selection message 8104, examines the digital signature, and transmits it to the service director processor. The service director processor updates the contents of an electronic ticket, or refunds the cost of the ticket in accordance with the reaction code 13002 contained in the reaction selection message 13007. When the user selects "refuse," the service director processor changes to the use disabled state the ticket status 4647 of the corresponding electronic ticket in the ticket list 4610 for the user, which is stored in the user information server 902.

[1729] When the reaction code 13002 represents "accept," in response to the modification request 8100, the service director processor generates a new electronic ticket using the same procedures as those used during the ticket purchase processing. In addition, the service director processor generates a modification instruction 13017, which is a message for instructing the modification of a ticket, and transmits it to the user processor. The user processor changes a corresponding electronic ticket in the user ticket list 4610 to an electronic ticket that is included in the modification instruction 13017. The user processor closes the modification instruction 13017 and addresses it to the user, and transmits it as a modification instruction 8105 to the mobile user terminal via digital wireless telephone communication.

[1730] As is shown in Fig. 130A, the digital signature of the service provider is provided for the data that consists of a modification reaction header 13011, which is header information indicating that the message is the modification instruction 8105 and describing the data structure; a modification number 13012; a request number 13013; new electronic ticket data 13014; a service provider ID 13015; and an issued time 13016, which indicates the date on which the modification instruction 8105 was issued. These data are closed and addressed to the user, thereby providing the modification instruction 8105.

[1731] Upon receiving the modification instruction 8105, the mobile user terminal decrypts it and examines the digital signature. Then, instead of the old electronic ticket, the mobile user terminal registers in the ticket list 1712 the new electronic ticket 13014 that is included in the modification instruction 8105, and displays the new electronic ticket on the LCD (display the ticket; 8106).

[1732] An explanation will now be given for the contents of the messages that are exchanged by the devices during the ticket refund processing.

[1733] In Fig. 82 are shown procedures for exchanging messages when the ticket refund processing is performed by immediate clearing. In Figs. 131A and 131B, 133A and 133B, and 134A and 134B are shown the contents of messages that are exchanged by the devices during the ticket refund processing. In Fig. 83 are shown procedures for exchanging messages when the ticket refund processing is performed by delayed clearing. In Figs. 131A and 131B, 132A and 132B, 133A and 133B, and 134A and 134B are shown the contents of messages that are exchanged by the devices.

[1734] The ticket refund process is performed when the user selects "refund" during in the ticket modification process (when the reaction code 13002 of the reaction selection message 13007 represents "refund"). Therefore, the message exchanging procedures up to the reaction selection 13007 are transmitted by the user processor to the service director processor, and the contents of those messages are the same as those employed for the ticket modification processing.

[1735] When the reaction code 13002 indicates "refund," the service director processor generates a refund request 13107, which is a message requesting that the ticket issuer refund the cost of the ticket. The ticket issuer processor closes the request 13107, addressing it to the ticket issuer, and transmits it as a refund request 8205 or 8305 to the ticket issuing system.

[1736] As is shown in Fig. 131A, the digital signature of the service provider is provided for the data that consist of a refund request header 13100, which is header information indicating that the message is a refund request and describing the data structure; a modification number 13101; a ticket ID 13102 for a ticket for which the cost is to be refunded; a request number 13103; a customer number 13104; a service provider ID

13105; and an issued time 13106, which indicates the date on which the refund request was issued. These data are closed and addressed to the ticket issuer, thereby providing the refund request 8205 or 8305.

[1737] Upon receiving the refund request 8205 or 8305, the ticket issuing server 1100 of the ticket issuing system updates data in the customer information server 1101, the ticket issuing information server 1102 and the ticket information server 1103, cancels the issued ticket, generates a refund commission 8206, which is a message requesting that the service providing system perform the refund process for an electronic ticket, and transmits the commission 8206 to the service providing system.

[1738] As is shown in Fig. 131B, the digital signature of the ticket issuer is provided for the data that consists of a refund commission header 13111, which is header information indicating that the message is the refund commission and describing the data structure; a transaction number 13112, which is an arbitrarily generated number that uniquely represents the ticket refund processing; a refund amount 13113; a clearing option 13114; a ticket ID 13115; a request number 13116; a ticket issuer ID 13117; and an issued time 13118, which indicates the date when the refund commission was issued. These data are closed and addressed to the service provider, thereby providing the refund commission 8206 or 8306.

[1739] The ticket issuer processor of the service providing system decrypts the received refund commission 8206 or 8306 and examines the digital signature, and transmits it to the service director processor. When the clearing option 13114 in the refund commission 13119 represents immediate clearing, the service director processor performs the refund process using immediate clearing. When the clearing option 13114 represents delayed clearing, the service director processor performs the ticket refund process using delayed clearing.

[1740] An explanation will now be given for the ticket refund process that uses immediate clearing.

[1741] In Fig. 82, upon receiving a refund commission 13119, the service director processor generates a refund clearing request 13222, which is a message requesting the performance of the refund clearing process. The transaction processor processor closes the request 13222 and addresses it to the transaction processor, and transmits it as a refund clearing request 8207 to the transaction processing system 106.

[1742] As is shown in Fig. 132B, the digital signature of the service provider is provided for the data that consists of a refund clearing request header 13212, which is header information indicating that the message is the refund clearing request 8207 and describing the data structure; a user clearing account 13213; a ticket issuer clearing account 13214, which indicates the clearing account of the ticket issuer; a refund amount 13215; a refund option code 13216; a request number 13217, which is issued by the mobile user terminal 100; a trans-

action number 13218, which is issued by the ticket issuing system; a validity term 13219, which specifies a period during which the refund clearing request 5904 is valid; a service provider ID 13220; and an issued time 13221, which indicates the date when the refund clearing request 5904 was issued. These data are closed and addressed to the transaction processor, thereby providing the refund clearing request 8207.

[1743] Upon receiving the refund clearing request 8207, the transaction server 1000 of the transaction processing system updates data in the subscriber information server 1001, the member store information server 102 and the transaction information server 103, performs the refund clearing process, and generates for the service providing system a refund clearing completion notification 8208 that is a message indicating that the refund clearing has been completed.

[1744] As is shown in Fig. 133A, the digital signature of the transaction processor is provided for the data that consists of a refund clearing completion notification header 13300, which is header information indicating that the message is the refund clearing notification 8208 and describing the data structure; a clearing number 13301, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 13302; a ticket issuer clearing account 13303; a refund amount 13304; a refund option code 13305; a request number 13306; a transaction number 13307; clearing information 13308 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 13309 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 13311; and an issued time 13312, which indicates the date when the refund clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the refund clearing completion notification 8208.

[1745] The transaction processor processor of the service providing system 110 decrypts the received refund clearing completion notification 8208 and examines the digital signature, and transmits the refund clearing completion notification 13313 to the service director processor. The service director processor employs the refund clearing completion notification 13313 to generate a refund clearing completion notification 13329 for the ticket issuer. The ticket issuer processor closes the notification 13329, addresses it to the ticket issuer, and transmits it as a refund clearing completion notification 8209 to the ticket issuing system 107.

[1746] As is shown in Fig. 133B, the digital signature of the service provider is provided for the data that consist of a refund clearing completion notification header 13317, which is header information indicating that the message is the refund clearing notification 8209 and describing the data structure; a clearing number 13318;

a customer number 13319; a ticket issuer ID 13320; a refund amount 13321; a clearing option 13322; a request number 13323; a transaction number 13324; clearing information 13325 for a ticket issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 13326; a service provider ID 13327; and an issued time 13328, which indicates the date when the refund clearing completion notification was issued. These data are closed and addressed to the ticket issuer, thereby providing the refund clearing completion notification 8209.

[1747] The ticket issuing system decrypts the received refund clearing completion notification 8209 and examines the digital signature, generates a refund receipt 8210, and transmits it to the service providing system.

[1748] As is shown in Fig. 134A, the digital signature of the ticket issuer is provided for the data that consists of a refund receipt header 13400, which is header information indicating that the message is the refund receipt 8210 and describing the data structure; a customer number 13201; refund information 13402; a refund amount 13403; a request number 13404; a transaction number 13405; a clearing number 13406; a transaction processor ID 13407; a ticket issuer ID 13408; and an issued time 13409, which indicates the date when the refund receipt 8210 was issued. These data are closed and addressed to the service provider, thereby providing the refund receipt 8210. The refund information 13402 concerns the refund process performed by the ticket issuing system, and is accompanied by the digital signature of the ticket issuer.

[1749] The ticket issuer processor of the service providing system 110 decrypts the received refund receipt 8210 and examines the digital signature, and transmits the refund receipt 13410 to the service director processor. The service director processor employs the refund receipt 13410 to generate a refund receipt 13421 to be transmitted to the user.

[1750] When the service director processor has transmitted the refund clearing completion notification 13329 to the ticket issuing system, the service director processor erases from the user ticket list 4610 stored in the user information server 902 the electronic ticket for which the refund was effected.

[1751] The user processor closes the refund receipt 13421, addressing it to the user, and transmits it as a refund receipt 8211 to the mobile user terminal 100 via digital wireless telephone communication.

[1752] As is shown in Fig. 134B, the digital signature of the service provider is provided for the data that consists of a refund receipt header 13414, which is header information indicating that the message is the refund receipt 8211 and describing the data structure; a user ID 13415; a decrypted refund receipt 13416 (13410); clearing information 13417 for a user that is accompanied by the digital signature of the transaction processor; refund information 13418; a service provider ID 13419; and an issued time 13420, which indicates the

date when the refund receipt 8211 was issued. These data are closed and addressed to the user, thereby providing the refund receipt 8211. The refund information 13418 concerns the electronic ticket refund process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1753] The mobile user terminal decrypts the received refund receipt 8211 and examines the digital signature, erases from the check list 1712 the electronic ticket for which the refund was effected, registers the refund receipt 13421 in the use list 1715, and displays the refund receipt 13421 on the LCD 303 (display the refund receipt; 8212).

[1754] An explanation will now be given for the ticket refund processing performed with the delayed clearing. In Fig. 83, the procedures up to the time the ticket issuing system transmits a refund commission to the service providing system are the same as are those for the immediate clearing.

[1755] When the delayed clearing is designated in accordance with the clearing option 13114, the service director processor generates a temporary refund receipt 13208 that corresponds to a temporary receipt for the refund process. The user processor closes the temporary refund receipt 13208, addressing it to the user, and transmits it as a temporary refund receipt 8307 to the mobile user terminal 100 via digital wireless telephone communication.

[1756] As is shown in Fig. 132A, the digital signature of the service provider is provided for the data that consist of a temporary refund receipt header 13200, which is header information indicating that the message is the temporary refund receipt 8307 and describe the data structure; a user ID 13201; refund information 13202; a refund amount 13203; a request number 13204; a transaction number 13205; a service provider ID 13206; and an issued time 13207, which indicates the date when the temporary refund receipt 8307 was issued. These data are closed and addressed to the user, thereby providing the temporary refund receipt 8307. The refund information 13202 concerns the electronic ticket refund process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1757] The mobile user terminal decrypts the received temporary refund receipt 8307 and examines the digital signature, erases the electronic ticket that is refund from the check list 1712, registers the temporary refund receipt 13208 to the use list 1715, and displays the temporary refund receipt 13208 on the LCD 303 (display the refund receipt; 8308).

[1758] The service director processor thereafter performs the refund clearing processing.

[1759] First, the service director processor generates the refund clearing request 13222, which is a message requesting the performance of the refund clearing process. The transaction processor processor closes the

request 13222, addressing it to the transaction processor, and transmits it as a refund clearing request 8309 to the transaction processing system 106.

[1760] The transaction processing system 106 decrypts the received refund clearing request 8309 and examines the digital signature, and performs the refund clearing process. Then, the transaction processing system 106 generates a refund clearing completion notification 8310, and transmits it to the service providing system 110.

[1761] The transaction processor processor of the service providing system 110 decrypts the received refund clearing completion notification 8310 and examines the digital signature, and transmits a refund clearing completion notification 13313 to the service director processor. The service director processor employs the refund clearing completion notification 13313 to generate the refund clearing completion notification 13329 for the ticket issuer. The ticket issuer processor closes the notification 13329, addressing it to the ticket issuer, and transmits it to the ticket issuing system 107 as a refund clearing completion notification 8311 for the ticket issuer.

[1762] The ticket issuing system decrypts the received refund clearing completion notification 8311 and examines the digital signature, and generates a refund receipt 8312 and transmits it to the service providing system.

[1763] The ticket issuer processor of the service providing system 110 decrypts the received refund receipt 8312 and examines the digital signature, and transmits a refund receipt 13410 to the service director processor. The service director processor employs the refund receipt 13410 to generate a refund receipt 13412 for the user.

[1764] The generated refund receipt 13412 is not immediately transmitted to the mobile user terminal 100 of the user, but when the mobile user terminal 100 performs the data updating process, the user processor replaces the temporary refund receipt 13208 in the use list 1715 with the refund receipt 13421, and transmits it as a part of the update data 8313 to the mobile user terminal 100.

[1765] The data structures of the refund clearing request 8309, the refund clearing completion notification 8310, the refund clearing completion notification 8311 and the refund receipt 8312 for the delayed clearing are the same as those used for the refund clearing request 8207, the refund clearing completion notification 8208, the refund clearing completion notification 8209 and the refund receipt 8210 for the immediate clearing.

[1766] The refund clearing process with the delayed clearing is not necessarily performed immediately after the temporary refund receipt is issued, and may be performed, for example, once a day with another clearing process.

[1767] An explanation will now be given for the con-

tents of messages that are exchanged by devices in various processes for electronic payment card service.

[1768] First, an explanation will be given for the contents of messages that are exchanged by devices during the payment card purchase processing.

[1769] In Fig. 61 are shown the procedures for the exchange of messages by devices during the payment card purchase processing. In Figs. 96A and 96B, 97A and 97B, 98A and 98B, 99A and 99B, and 100A and 100B are shown the contents of messages that are exchanged by devices during the payment card purchase processing.

[1770] First, when a user performs a payment card purchase order operation 6100, the mobile user terminal transmits a payment card purchase order 6101 to the service providing system through digital wireless telephone communication.

[1771] As is shown in Fig. 96A, the digital signature of a user is provided for data that consists of a payment card purchase order header 9600, which is header information identifying the message as the payment card purchase order 6101 and describing the data structure; a response code 9601, which identifies the type of service requested by the user; a card order code 9602, which identifies an order code for a payment card that is entered by the user; a number of payment cards 9603 that the user has entered; a payment service code 9604, which identifies a credit card designated by the user; a payment value 9605; a payment option code 9606, which identifies a payment option, such as the number of payments designated by the user; a request number 9607, which is an arbitrarily generated number that uniquely represents the payment card purchase processing; a validity term 9608 for the payment card purchase order 6101; a user ID 9609; and an issued time 9610, which is the date on which the payment card purchase order 6101 was issued. These data are closed and addressed to the service provider, thereby providing the payment card purchase order 6101. The service code 8901 identifies the purchase order of a payment card to a payment card issuer who is selected by the user.

[1772] Upon receiving the payment card purchase order 6101, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group that processes a payment card order 9611. The service director processor refers to the payment card issuer list 5204 and generates a payment card purchase order 9626 for the payment card issuer indicated by the service code 9601. The payment card issuer processor closes the payment card order and addresses it to the payment card issuer, and transmits the resultant order as a payment card purchase order 6102 to the payment card issuing system 108.

[1773] As is shown in Fig. 96B, the digital signature of

a service providing system is provided for data that consists of a payment card purchase order header 9615, which is header information indicating that the message is the payment card purchase order 6102 and describing the data structure; a card order code 9616; a number of cards 9617 that are purchased; a payment service code 9618; a payment value 9619; a payment option code 9620; a request number 9621; a customer number 9622, which uniquely represents a user for the payment card issuer; a validity term 9623 for the payment card purchase order 6102; a service provider ID 9624; and an issued time 9625, which is the date on which the payment card purchase order 6102 was issued. These data are closed and addressed to the payment card issuer, thereby providing the payment card purchase order 6102.

[1774] When there was a previous transaction to which the user and the payment card issuer were parties, a customer number that is registered in the customer table of the payment card issuer is established as the customer number 9622. When there was no previous transaction, the service director processor generates for the payment card issuer a number that uniquely represents the user, establishes it as the customer number 9622, and registers that number in the customer table. The customer table is designated by using the customer table address 5237 of the payment card issuer list 5204.

[1775] Upon receiving the payment card purchase order 6102, the payment card issuing system 108 decrypts it and examines the digital signature. The payment card issuing server 1200 updates the data in the customer information server 1201, the payment card issuing information server 1202 and the payment card information server 1203, generates payment card data (9719) for the ordered payment card, and transmits, to the service providing system, an electronic payment card issuing commission 6103, which constitutes a message requesting the process for issuing an electronic payment card that corresponds to the payment card and the process for settling the price of the payment card.

[1776] As is shown in Fig. 97A, the digital signature of a payment card issuer is provided for data that consists of an electronic payment card issuing commission header 9700, which is header information identifying the message as the electronic payment card issuing commission 6103 and describing the data structure; a transaction number 9701, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 9702, which conveys the price of a payment card; a clearing option 9703, which indicates which clearing procedures apply; a request number 9704; a payment card code 9705, which identifies the type of electronic payment card that is to be issued; a template code 9706, which identifies a template program to be used for an electronic payment card that is to be issued; a number of payment cards 9707,

which indicates how many payment cards are to be issued; payment card data 9708; representative component information 9709; a payment card issuer ID 9710; and an issued time 9711, which is the date on which the electronic payment card issuing commission 6103 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card issuing commission 6103.

[1777] The clearing option 9703 is information by which the payment card issuing system designates, to the service providing system, the procedures to be used for clearing the price of a payment card. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic payment card to a user after the price of the payment card has been cleared, and a delayed clearing process for clearing the price of a payment card after an electronic payment card has been issued. The clearing option 9703 is used to designate either clearing process.

[1778] In the delayed clearing process, since an electronic payment card is issued to a user before the clearing process is performed, the user does not have to wait.

[1779] For example, based on a purchase history maintained for customers, the payment card issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known to be trustworthy, and can designate the spontaneous clearing for a customer with whom it has had no previous dealings.

[1780] The payment card data 9708 is payment card information issued by the payment card issuer. A number of payment card information items equivalent to the number of payment cards 9707 are established as the payment card data 9708. For one payment card, the digital signature of a payment card issuer is provided for data that consist of a card ID 9716, card information 9717 and a payment card issuer ID 9718, and the payment card information is thereby provided. The payment card information 9717 is ASCII information describing the contents of a payment card. For the payment card information 9717, the title of a payment card, the face value of the payment card that is issued, the usage condition, an issuer, and whether it can be transferred, are described using a form whereby tag information representing information types is additionally provided.

[1781] The representative component information 9709 is information that is established as the representative component information 2032 for an electronic payment card to be generated. Therefore, the representative component information 9709 may not be set for use.

[1782] The payment card issuer processor of the service providing system receives the electronic payment card issuing commission 6103, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic payment card issuing process and

the payment card price clearing process in accordance with the clearing procedures designated by using the clearing option 9703.

[1783] In Fig. 61 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1784] For the spontaneous clearing, the service director processor generates a clearing request 9824, which is a message requesting the clearing of the price of a payment card. The transaction processor processor closes the clearing request 9824 and addresses it to the transaction processor, and then transmits it as a clearing request 6104 to the transaction processing system 106.

[1785] As is shown in Fig. 98B, the digital signature of a service provider is provided for data that consists of a clearing request header 9814, which is header information indicating that the message is the clearing request 6104 and describing the data structure; a user clearing account 9815, which includes a credit card that corresponds to the payment service code designated by the user; a payment card issuer clearing account 9816, which designates the clearing account of a payment card issuer; a payment value 9817; a payment option code 9818; a request number 9819, which is issued by the mobile user terminal 100; a transaction number 9820, which is issued by the payment card issuing system; a validity term 9821, which presents the period during which the clearing request 6104 is effective; a service provider ID 9822; and an issued time 9823, which indicates the date on which the clearing request 6104 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 6104.

[1786] The transaction processing system 106 receives the clearing request 6104, decrypts it and examines the digital signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 6105, and transmits it to the service providing system 110.

[1787] As is shown in Fig. 99A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 9900, which is header information indicating that the message is the clearing completion notification 6105 and describing the data structure; a clearing number 9901, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 9902; a payment card issuer clearing account 9903; a payment value 9904; a payment option code 9905; a request number 9906; a transaction number 9907; clearing information 9908 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 9909 for a payment card issuer that is accompanied by the digital signature of the transaction processor; clearing information 9910 for a user that is accompanied by the digital signature of the trans-

action processor; a transaction processor provider ID 9911; and an issued time 9912, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 6105.

[1788] Upon receiving the clearing completion notification 6105, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9913 to the service director processor. Upon receiving the clearing completion notification 9913, the service director processor generates a clearing completion notification 9930 for the payment card issuer. The payment card issuer processor closes the clearing completion notification 9930, and transmits it to the payment card issuing system 107 as a clearing completion notification 6106 for the payment card issuer.

[1789] As is shown in Fig. 99B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 9917, which is header information indicating that the message is the clearing completion notification 6106 and describing the data structure; a clearing number 9918; a customer number 9919; a payment card issuer ID 9920; a payment service code 9921; a payment value 9922; a payment option code 9923; a request number 9924; a transaction number 9925; clearing information 9926 for a payment card issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 9927; a service provider ID 9928; and an issued time 9929, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the payment card issuer, thereby providing the clearing completion notification 6106.

[1790] Upon receiving the clearing completion notification 6106, the payment card issuing system decrypts it and examines the digital signature, and generates a receipt 6107 and transmits it to the service providing system.

[1791] As is shown in Fig. 100A, the digital signature of a payment card issuer is provided for data that consists of a receipt header 10000, which is header information indicating that the message is the receipt 6107 and describing the data structure; a customer number 10001; payment card issuing information 10002; a payment service code 10003; a payment value 10004; a payment option code 10005; a request number 10006; a transaction number 10007; clearing information 10008; a transaction processor ID 10009; a payment card issuer ID 10010; and an issued time 10011, which indicates the date on which the receipt 6107 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 6107. The payment card issuing information 10002 is information concerning the payment card issuing process per-

formed by the payment card issuing system, and is accompanied by the digital signature of the payment card issuer.

[1792] Upon receiving the receipt 6107, the payment card issuer processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 10012 to the service director processor. The service director processor employs the receipt 10012 to generate a receipt 10023 for a user.

[1793] In addition, the service director processor generates a clearing completion notification 9930 for the payment card issuing system, generates an electronic payment card to be issued to the user, and further generates an electronic payment card issuing message 9227 that includes the electronic payment card that is generated.

[1794] The user processor closes the electronic payment card issuing message 9227 and the receipt 10023 while addressing them to the user, and transmits them as an electronic payment card issuing message 6108 and a receipt 6109 to the mobile user terminal 100 via digital wireless communication.

[1795] As is shown in Fig. 97B, the digital signature of a service provider is provided for data that consist of an electronic payment card issuing header 9720, which is header information indicating that the message is the electronic payment card issuing message 6108 and describing the data structure; a transaction number 9721; a request number 9722; the number of payment cards 9723; electronic payment card data 9724 that are generated; a service provider ID 9725; and an issued time 9726, which indicates the date on which the electronic payment card issuing message 6108 was issued. These data are closed and addressed to the user, thereby providing the electronic payment card issuing message 6108. The electronic payment card data 9724 includes electronic payment cards 9731 equivalent in number to the number of payment cards 9723.

[1796] As is shown in Fig. 100B, the digital signature of a service provider is provided for data that consists of a receipt header 10016, which is header information indicating that the message is the receipt 6109 and describing the data structure; a user ID 10017; a receipt 10018 (10012) obtained by decryption; clearing information 10019 for a user that is accompanied by the digital signature of a transaction processor; payment card issuing information 10020; a service provider ID 10021; and an issued time 10022, which indicates the date on which the receipt 6109 was issued. These data are closed and addressed to the user, thereby providing the receipt 6109. The payment card issuing information 10020 is information for the electronic payment card issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1797] Upon receiving the electronic payment card issuing message 6108 and the receipt 6109, the mobile user terminal decrypts them and examines the digital

signatures, enters in the payment card list 1713 an electronic payment card included in the electronic payment card issuing message 6108, enters the receipt 10023 in the use list 1715, and displays the electronic payment card on the LCD 303.

[1798] The generation of an electronic payment card by the service director processor is performed as follows.

[1799] First, the service director processor refers to the electronic payment card template list 5005 for the payment card issuer that is stored in the payment card issuer information server. Then, by using the electronic payment card template program that is identified by the template code 9706 of the electronic payment card issuing commission 6103, the service director processor generates a payment card program for an electronic payment card. Specifically, the payment card program data 2013 for an electronic payment card are generated using the transaction module and the representation module, which are described as being located at the transaction module address 5019, and the representation module address 5020 in the electronic payment card template list 5005, and the representative component information 9709 in the electronic payment card issuing commission 6103. When the representative component information 9709 is not present in the electronic payment card issuing commission 6103, the default representative component information located at the default representative component information address 5021 is employed as the information for an electronic payment card.

[1800] Following this and based on the payment card information included in the card information 9717, the service director processor generates the card status 2007 and the total remaining value 2008. Whether the card status 2007 can be transferred is designated, and the face value of the payment card that is issued is set as the total remaining value 2007. The service director processor generates a new pair consisting of a card signature private key and a card signature public key, and further generates the payment card program 2001 for an electronic payment card by employing the card private key and the accounting machine public key that are registered in the electronic payment card management information 5400.

[1801] Furthermore, the service director processor generates an electronic payment card by employing the obtained card signature public key to generate the certificate 2003 for the electronic payment card, and by employing the payment card data 9719 in the electronic payment card issuing commission 6103 to generate the presentation card 2002 for the electronic payment card.

[1802] The procedures for the delayed clearing will now be described.

[1803] In Fig. 62 are shown the procedures for exchanging messages between the devices in the payment card purchase process for the delayed clearing. The same process is performed as is used for the spon-

taneous clearing until the payment card issuing system transmits the electronic payment card issuing commission to the service providing system.

[1804] When the delayed clearing is designated by the clearing option 9703, the service director processor generates an electronic payment card to be issued to the user, and also generates the electronic payment card issuing message 9727, which includes the generated electronic payment card, and a temporary receipt message 9810, which corresponds to a temporary receipt. The generation of the electronic payment card is performed in the same manner as that used for the spontaneous clearing.

[1805] The user processor closes the electronic payment card issuing message 9727 and the temporary receipt 9810 and addresses them to the user, and transmits these messages as an electronic payment card issuing message 6204 and a temporary receipt 6205 to the mobile user terminal 100 via digital wireless telephone communication.

[1806] As is shown in Fig. 98A, the digital signature of a service provider is provided for data that consists of a temporary receipt header 9800, which is header information indicating that the message is the temporary receipt 6205 and describing the data structure; a user ID 9801; payment card issuing information 9802; a payment service code 9803; a payment value 9804; a payment option code 9805; a request number 9806; a transaction number 9807; a service provider ID 9808; and an issued time 9809, which indicates the date on which the temporary receipt 6205 was issued. These data are closed and addressed to the user, thereby providing the temporary receipt 6205. The payment card issuing information 9802 is information concerning the electronic payment card issuing process that is performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1807] The data structure of the electronic payment card issuing message 6204 is the same as that used for the electronic payment card issuing message 6108.

[1808] Upon receiving the electronic payment card issuing message 6204 and the temporary receipt 6205, the mobile user terminal decrypts them and examines the digital signatures, enters an electronic payment card included in the electronic payment card issuing message 6204 in the payment card list 1713, enters the temporary receipt 9810 in the use list 1715, and displays the electronic payment card on the LCD 303.

[1809] Following this, the service director processor performs the clearing process for the price of the payment card. First, the service director processor generates a clearing request 9824, which is a message requesting the performance of the clearing process for the price of the payment card. The transaction processor closes the clearing request 9824 and addresses it to the transaction processor, and transmits it as a clearing request 6207 to the transaction processing system 106.

[1810] Upon receiving the clearing request 6207, the

transaction processing system 106 decrypts it and examines the digital signature, and performs the clearing process. The transaction processing system 106 generates a clearing completion notification 6208 and transmits it to the service providing system 110.

[1811] Upon receiving the clearing completion notification 6208, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 9913 to the service director processor. The service director processor employs the received clearing completion notification 9913 to generate a clearing completion notification 9930 for the payment card issuer. And the payment card issuer processor closes the clearing completion notification 9930 and transmits it to the payment card issuing system 108 as a clearing completion notification 6209 for the payment card issuer.

[1812] The payment card issuing system decrypts the received clearing completion notification 6209 and examines the digital signature, and generates a receipt 6210 and transmits it to the service providing system.

[1813] The payment card issuer processor of the service providing system decrypts the received receipt 6210 and examines the digital signature, and transmits a receipt 10012 to the service director processor. The service director processor employs the receipt 10012 to generate a receipt 10023 for a user.

[1814] The receipt 10023 that is generated is not immediately transmitted to the mobile user terminal 100 of the user. When the mobile user terminal has performed the data updating process, the user processor replaces the temporary receipt 9810 in the use list 1715 with the receipt 10023, and transmits the receipt 10023 as one part of the update data 6211 to the mobile user terminal 100.

[1815] The data structures of the clearing request 6207, the clearing completion notification 6208, the clearing completion notification 6209 and the receipt 6210 for the delayed clearing are the same as those provided for the clearing request 6104, the clearing completion notification 6105, the clearing completion notification 6106 and the receipt 6107 for the spontaneous clearing.

[1816] The delayed clearing process need not be performed immediately after the electronic payment card is issued, and together with the other clearing processes, may be performed, for example, once a day.

[1817] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110 during the payment card registration processing.

[1818] In Fig. 65B are shown the procedures for exchanging messages between devices in the payment card registration processing, and in Figs. 107A and 107B are shown the contents of messages that are exchanged by the devices in the payment card registration processing.

[1819] First, when the user performs an electronic payment card registration operation 6504, the mobile user terminal generates a payment card registration request 6505 and transmits it to the service providing system via digital wireless telephone communication.

[1820] As is shown in Fig. 107A, the digital signature of a user is provided for data that consists of a payment card registration request header 10700, which is header information indicating that the message is the payment card registration request 6505 and describing the data structure; a card ID 10701 of a payment card to be registered; a user ID 10702; and an issued time 10703, which indicates the date on which the payment card registration request 6505 was issued. These data are closed and addressed to the service provider, thereby providing the payment card registration request 6505.

[1821] The user processor of the service providing system decrypts the received payment card registration request 6505 and examines the digital signature, and transmits the request 6505 to the service manager processor. The service manager processor generates a service director processor to form a process group that processes a payment card registration request 10704. The service director processor ascertains that the electronic payment card indicated by the card ID 10701 is registered in the payment card list 4611 for the user in the user information server 902, and registers that electronic payment card in the registered card list 5402 for electronic payment cards of the service director information server 901. At this time, the service director processor newly generates a card signature private key and a card signature public key pair. Further, the service director processor generates a registered card certificate using the card signature public key, and registers it in the registered card list 5402. The service director processor then generates a card certificate issuing message 10713 using the card signature private key and the registered card certificate that has been generated. The user processor closes the card certificate issuing message 10713 and addresses it to the user, and transmits it as a payment card certificate issuing message 6506 to the mobile user terminal via digital wireless telephone communication.

[1822] As is shown in Fig. 107B, the digital signature of a service provider is provided for data that consists of a card certificate issuing header 10708, which is header information indicating that the message is the payment card certificate issuing message 6506 and describing the data structure; a card digital signature private key 10709; a registered card certificate 10710; a service provider ID 10711, and an issued time 10712, which indicates the date on which the payment card certificate issuing message 6506 was issued. These data are closed and addressed to the user, thereby providing the payment card certificate issuing message 6506.

[1823] The mobile user terminal 100 decrypts the received payment card certificate issuing message 6506 and examines the digital signature, replaces the

card signature private key and the card certificate of an electronic payment card with the card signature private key 10709 and the registered card certificate 10710, both of which are included in the payment card certificate issuing message 6506, changes the registration state in the card status to the post-registration state, and displays on the LCD the electronic payment card that has been registered (display a payment card that is registered; 6507).

[1824] An explanation will now be given for the contents of messages that are exchanged by the service providing system 110 and the merchant terminal 102, the merchant terminal 103, or the accounting machine 3555 (automatic vending machine 104) during the payment card setup processing.

[1825] The payment card setup processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1826] Therefore, for the payment card setup process, the procedures for the exchange of messages by the service providing system and the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and the contents (data structures) of the messages to be exchanged are the same as those used for the above described data updating processing (Figs. 57 and 88).

[1827] It should be noted, however, that the payment card setup process is not performed each time the data updating process is performed, but when the payment card list 4609 for the merchant stored in the merchant information server 903 is updated by the service director processor.

[1828] When the payment card list 4609 is updated, the merchant processor includes updated data in the payment card list 4609 for the compressed update data 8828 in the update data 5705, and transmits the resultant data as update data 5705 to the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1829] Upon receiving the update data 5705, the merchant terminal 102 (the merchant terminal 103 or the accounting machine 3555) decompresses the update data 8828, and updates the data in the RAM and on the hard disk. At this time, the payment card list 2811 (3211 or 3608) in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) is updated, and an electronic payment card that is handled by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) is updated.

[1830] An explanation will now be given for the contents of messages that are exchanged by between the mobile user terminal 100 and the merchant terminal 102, the merchant terminal 103, or the accounting machine 3555 (automatic vending machine 104) during the payment card clearing processing.

[1831] In Fig. 68 are shown procedures for the exchange of messages by the mobile user terminal 100 and the merchant terminal 102 or 103 during the payment card clearing processing, and in Fig. 69 are shown procedures for the exchange of by the mobile user terminal 100 and the accounting machine 3555. In Figs. 112A and 112B and Figs. 113A and 113B are shown the contents of messages that are exchanged by the devices during the payment card clearing processing. For the payment card clearing processing, the same procedures are employed for the exchange of messages by the mobile user terminal 100 and the merchant terminal 102, the merchant terminal 103 or the accounting machine 3555, and the same contents (data structures) are included in the messages to be exchanged.

[1832] First, when a user performs a payment offer operation 6804 or 6906, the mobile user terminal employs a payment card that is to be used for payment and an arbitrarily generated test pattern and produces a payment offer message 6805 or 6907, which is a message for offering the merchant the payment of a price. The mobile user terminal transmits the message 6805 or 6907 to the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) via infra-red communication.

[1833] As is shown in Fig. 112A, the payment offer message 6805 or 6907 consists of a payment offer header 11200, which is header information indicating that the message is the payment offer message 6805 or 6907 and describes the data structure; a service code 11201, which identifies the request for payment using an electronic payment card; a request number 11202, which is an arbitrarily generated number that uniquely represents the payment card clearing process; an amount of payment 11203 that is entered by the user; a presentation card 11203 for presenting an electronic payment card to be used for the payment; a card certificate 11205; a current card status 11206 for an electronic payment card to be used for the payment; a total remaining value 11207; a card ID 11208; an issued time 11209, which indicates the date on which the payment offer message 6805 or 6907 was issued; and an accounting machine test pattern 11211, which is an arbitrarily generated test pattern. The digital signature is provided, using the card signature private key of an electronic payment card, for the card status 11206, the total remaining value 11207, the card ID 11208 and the issued time 11209. The accounting machine test pattern 11211 is encrypted using the accounting machine public key.

[1834] The presentation card 11204, the card certificate 11205, the card status 11206, the total remaining value 11207, the card ID 11208 and the issued date 11209 specify the contents of the electronic payment card for the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and the accounting machine test pattern 11211 is a test pattern

for authorizing the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1835] Upon receiving the payment offer 6805 or 6907, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) refers to the payment card list 2811 (3211 or 3608) and activates a payment card clearing module that corresponds to the card code (included in a presentation card) for the electronic payment card that is presented. Then, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) examines the validity of the contents of the payment offer 6805 or 6907, generates a payment offer response 6806 or 6908, which is a response message for the payment offer, and transmits it to the mobile user terminal via infrared communication. When the electronic payment card that is presented is not registered in the payment card list 2811 (3211 or 3608), the payment offer response 6806 or 6907 is transmitted, which indicates that the pertinent electronic payment card is not available.

[1836] In the verification processing for determining the validity of the payment offer message 6805 or 6907, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) verifies that for the sale the amount of payment 11203 designated by the user is adequate. The merchant terminal 102 employs the fact that the card certificate 11205 is a registered card certificate, and examines the card status 11206 and the total remaining value 11207 to determine whether the electronic payment card is valid and can be used as a payment card for the payment. Then, the merchant terminal 102 examines the presentation card 11204, the digital signature of the service provider that is provided for the card certificate 11205, and the validity term. Further, the merchant terminal employs the card signature public key of the card certificate 11205 to examine the digital signature of the electronic payment card that is provided for the card status 11206, the total remaining value 11207, the card ID 11208 and the issued time 11209. In this fashion, the validity of the payment offer 6805 or 6907 is verified.

[1837] In the generation of the payment offer response 6806 or 6908, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) decrypts the accounting machine test pattern 11211 using the accounting machine private key, and employs the card public key to encrypt the card test pattern 11211 that is arbitrarily generated.

[1838] As is shown in Fig. 112B, the digital signature of a merchant is provided for the data that consists of a payment offer response header 11213, which is header information indicating that the message is the payment offer response 6806 or 6908 and describing the data structure; a transaction number 11214; a response message 11215; a request number 11216; a card ID 11217; an instruction code 11218; an amount of sales 11219, which indicates the price that is charged or the cost of the service that is calculated by the merchant

terminal 102 (or the merchant terminal 103 or the accounting machine 3555); an accounting machine test pattern 11220, which is decrypted; a card test pattern 11221, which is an arbitrarily generated test pattern; an accounting machine ID 11223; a merchant ID 11224; and an issued time 11225, which indicates the date on which the payment offer response 6805 or 6908 was issued. In this fashion, the payment offer response 6806 or 6908 is provided. The card test pattern 11221 is encrypted using the card public key.

[1839] The transaction number 11214 is a number that is arbitrarily generated, by the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), and that uniquely represents the payment card clearing process. When, as a result of the examination of the payment offer 6805 or 6907, the payment card clearing process can not be performed (the amount of the payment entered by the user is not sufficient, or when an electronic payment card is one that can not be handled by the pertinent merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555)), a value of 0 is set. When the payment card clearing process can be performed, a value other than 0 is set.

[1840] The response message 11215 is text information constituting the message transmitted by the merchant to the user. When the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) can not handle an electronic payment card that has been presented (transaction number = 0), data to that effect is included in the response message. The response message is prepared optionally, and may not be prepared.

[1841] The instruction code 11218 is command code information for an electronic payment card, and is used when a value equivalent to the amount of sales 11219 is subtracted from the total remaining value held by the electronic payment card. The instruction code is varied by combining the electronic payment card transaction module and the payment card clearing module.

[1842] When the mobile user terminal receives the payment offer response 6806 or 6908, first, for verification of to verify the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555), it compares the accounting machine test pattern 11211 with the accounting machine test pattern 11220 included in the payment offer response 6806 or 6908. The mobile user terminal ascertains whether the amount of sales 11219 is equal to or smaller than the amount of payment 11203 entered by the user, and subtracts the amount of sales 11219 from the total remaining value held by the electronic payment card in accordance with the instruction code 11218. Then, the mobile user terminal decrypts the card test pattern using the card private key, and generates a micro-check message 6807 or 6909, which corresponds to a check that has as its face value the amount of the sale. The check is transmitted via infrared communication to the mer-

chant terminal 102 (or to the merchant terminal 103 or the accounting machine 3555).

[1843] As is shown in Fig. 113A, the digital signature using the card signature private key and the digital signature of a user are provided for the data that consists of a micro-check header 11300, which is header information indicating that the message is the micro check 6807 or 6909 and describing the data structure; a micro-check issuing number 11301, which indicates the order of the payment card clearing process; a card test pattern 11302, which is decrypted; an amount of payment 11303, which indicates the obtained value that is subtracted from the total remaining value; a card status 11304; a total remaining value 11305 available after the subtraction; an accounting machine ID 11306; a merchant ID 11307; a request number 11308; a transaction number 11309; a card code 11310; a card ID 11311; and an issued time 11312, which indicates the date on which the micro-check 6807 or 6909 was issued. In this fashion, the micro-check 6807 or 6909 is provided.

[1844] Upon receiving the micro-check 6807 or 6909, first, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) authorizes the electronic payment card by comparing the card test pattern 11221 with the card test pattern 11302 that is included in the micro-check 6807 or 6909, examines the validity of the contents of the micro-check 6807 or 6909, and generates a receipt 6808 or 6910 and transmits it to the mobile user terminal via infrared communication.

[1845] In the verification process for the validity of the micro-check 6807 or 6909, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) determines whether the amount of payment 11303 represented by the micro-check 6807 or 6909 is adequate for the value of the sale. Also, the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) determines whether the value obtained by subtracting the total remaining value 11305 from the total remaining value 11207, which represents the payment offer, is equal to the amount of payment 11303 represented by the micro-check. Finally, the merchant terminal 102 examines the digital signature of the electronic payment card accompanying the micro-check 6807 or 6909.

[1846] As is shown in Fig. 113B, the digital signature of a merchant is provided for the data that consists of a receipt header 11314, which is header information indicating that the message is the receipt 6808 or 6910 and describing the data structure; sales information 11315; a card ID 11316; a total receipt value 11317, which indicates the same value as the amount of payment 11303 represented by the micro-check that is received by the merchant; a request number 11318; a transaction number 11319; a micro-check issuing number 11320; an accounting machine ID 11321; a merchant ID 11322; and an issued time 11323, which indicates the date on which the receipt 6808 or 6910 was issued. In this fashion, the receipt 6808 or 6910 is provided.

[1847] The sales information 11315 is text information constituting the contents of a transaction acquired during the payment card clearing process, and corresponds to the specifications for the products that are traded or for the service that is provided, or for a statement of account.

[1848] Upon receiving the receipt 6808 or 6910, the mobile user terminal verifies that the total receipt value 11317 is equal to the amount of payment 11303 of represented by the micro-check, and increments the micro-check issuing number. The mobile user terminal then registers the receipt 6808 or 6910 as usage information in the use list 1715, and displays the receipt 6808 or 6910 on the LCD (display the receipt; 6810 or 6911).

[1849] When the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555) has transmitted the receipt 6808 or 6910, it registers, in the transaction list 2812 (3212 or 3609), the micro-check 6807 or 6909 and the receipt 6808 or 6910 as history information for the payment card clearing process.

[1850] The merchant terminal 102 or the merchant terminal 103 displays, on the LCD, a message that indicates the termination of the payment card clearing process (display the clearing completion; 6809), and the product is delivered by the merchant to the user (deliver the product; 6811). Thereafter, the accounting machine 3555 (automatic vending machine 104) discharges the product to the discharge port 703.

[1851] When the mobile user terminal receives the payment offer, and the amount of payment 11203 entered by the user is greater than the amount of sales 11219, the dialogue message for asking the user for the value of the payment is displayed on the LCD 303. When the user again enters a payment value that is greater than the amount of sales 11219, a micro-check having the entered value as the payment value 11303 may be issued. In this case, a value that corresponds to the difference between the amount of payment 11303 and the amount of sales 11219 can be paid as a commission to the merchant.

[1852] An explanation will now be given for the contents of messages that are exchanged by the devices during the payment card reference processing.

[1853] In Fig. 72 are shown procedures for the exchange of messages by the devices during the payment card reference processing, and in Figs. 88A to 88D and Fig. 116B are shown the contents of messages that are exchanged during the payment card reference processing. The payment card reference processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555).

[1854] Therefore, for the payment card reference process, the procedures for the exchange of messages by the merchant terminal 102 (or the merchant terminal

103 or the accounting machine 3555) and the service providing system, and the contents (data structures) of the messages to be exchanged are the same as those employed for the above described data updating processing.

[1855] Compressed upload data 8818 in the upload data 5702 include a micro-check that is newly registered in the transaction list 2510 during the payment card clearing process conducted during the period extending from the previous performance of the data updating process to the current performance of the data updating process.

[1856] During the data updating processing, the merchant processor transmits, to the service manager processor, a message requesting the reference process be performed for the micro-check that is uploaded from the merchant terminal 102 (or the merchant terminal 103 or the accounting machine 3555). The service manager processor generates a service director processor to form a process group for examining the validity of the micro-check.

[1857] First, the service director processor determines whether the accounting machine ID 11306 and the merchant ID 11307 in the micro-check match the accounting machine ID 5215 of the merchant and the merchant ID 5214. Then, the service director processor examines the registered card list 5402 in the service director information server 901 to verify that the electronic payment card for which the micro-check was issued is registered. The service director processor employs the user public key 5419 to examine the digital signature of the user that accompanies the micro-check, and employs the registered card certificate to examine the digital signature for the payment card that accompanies the micro-check. In addition, the service director processor employs the micro-check issuing number when examining the matching of the amount of payment with the total remaining value, and transmits the result of the examination to the merchant processor. As a result, the micro-check is registered in the micro-check list.

[1858] The merchant processor enters the received payment card reference results in the compressed update data 8828 in the update data 5705, and transmits the data 5705 to the merchant terminal 102 (or the merchant terminal 103).

[1859] When an error occurs in the process for verifying the validity of the micro-check, the service director processor transmits a message indicating that an error occurred in the management system 908.

[1860] Upon receiving the update data 5705, the merchant terminal 102 (or the merchant terminal 103) decompresses the update data 8828 and updates the data in the RAM and on the hard disk. At this time, the payment card reference results are registered in the authorization report list 2813 (3213) of the merchant terminal 102 (the merchant terminal 103).

[1861] If the firm represented by the merchant differs from that represented by the payment card issuer, and a

payment for the merchant who handles the payment card is made by the payment card issuer, or if the usage of the payment card is periodically reported to the payment card issuer in accordance with the terms of a contract, in accordance with the micro-check that is newly registered in the micro-check list, the service director processor generates weekly, for example, a usage condition notification 11616, which is a message for notifying the payment card issuer of the payment card usage condition. The payment card issuer processor closes the notification 11616 and addresses it to the payment card issuer, and transmits it as a usage report 7200 to the payment card issuing system 108.

[1862] As is shown in Fig. 116B, the digital signature of a service provider is provided for the data that consists of a usage report header 11610, which is header information indicating that the message is the usage report 7200 and describing the data structure; a card ID and payment value list 11611 of payment cards that are employed; the merchant name 11612 and the merchant ID 11613 of a merchant that handles the payment card; a service provider ID 11614; and an issued time 11615, which indicates the date on which the usage report 7200 was issued. These data are closed and addressed to the payment card issuer, thereby providing the usage report 7200.

[1863] Upon receiving the usage report 7200, the payment card issuing system 108 decrypts it and examines the digital signature, and performs such processing as making a payment to the merchant.

[1864] An explanation will now be given for the contents of messages that are exchanged by the devices during the payment card transfer processing.

[1865] In Fig. 75 are shown procedures for the exchange of messages by the devices during the payment card transfer processing, and in Figs. 120A and 120B, 121A and 121B, and 122A and 122B are shown the contents of messages that are exchanged during the payment card transfer processing.

[1866] The payment card transfer process can be performed when the card status 2007 of the electronic payment card indicates the transfer enabled state, which is designated by the payment card issuer when issuing a payment card.

[1867] In Fig. 75 is shown a case where user A transfers an electronic payment card to user B. The procedures for the exchange of messages by the devices belonging to users A and B are the same for infrared communication as they are for digital wireless communication. The data structures of messages are also the same.

[1868] In Fig. 75, first, when user A performs a payment card transfer process 7500, the mobile user terminal of user A transmits a payment card transfer offer 7501, which is a message offering to transfer an electronic payment card, to the mobile user terminal of user B. When at this time the mobile user terminals of user A and user B are connected, communication between

user A and user B is performed via digital wireless telephone. When the mobile user terminals are not connected, infrared communication is employed.

[1869] As is shown in Fig. 120A, the digital signature of user A is provided for the data consisting of a card transfer offer header 12000, which is header information indicating that the message is the card transfer offer 7501 and describing the data structure; a transfer offer number 12001, which is an arbitrarily generated number that uniquely represents the payment card transfer process; a presentation card 12002 and a card certificate 12003 for an electronic payment card to be transferred; a card status 12004; a total remaining value 12005; a card ID 12006; an issued time 12007, which indicates the date on which the card transfer offer 7501 was issued; and a user public key certificate 12009. In this fashion, the card transfer offer 7501 is provided. The digital signature of the electronic payment card is provided, using the card signature private key, for the card status 12004, the variable card information 12005, the card ID 12006 and the issued time 12007.

[1870] The digital signature of the service provider is provided for the data that consist of a user public key header 12010; the user public key 12011 of user A; a public key certificate ID 12012, which is ID information for the public key certificate; a certificate validity term 12013; a service provider ID 12014; and a certificate issued time 12015. In this fashion, the user public key certificate 12009 is provided.

[1871] Upon receiving the card transfer offer 7501, the mobile user terminal of user B examines the presentation card 12002, the card certified 12003, and the digital signature of the service provider and the validity term of the public key certificate 12009. Then, the mobile user terminal examines the digital signature of the electronic payment card that is provided for the card status 12004, the total remaining value 12005, the card ID 12006 and the issued time 12007, and the digital signature of user A accompanying the card transfer offer 7501, and verifies the contents of the card transfer offer 7501. In accordance with the presentation card 12002, the card status 12004 and the total remaining value 12005, the mobile user terminal then displays, on the LCD, the contents of the electronic payment card that is to be transferred (display the transfer offer; 7502).

[1872] When user B performs a transfer offer acceptance operation 7503, the mobile user terminal of user B transmits, to the mobile user terminal of user A, a card transfer offer response 7504, which is a response message for the card transfer offer 7501.

[1873] As is shown in Fig. 120B, the digital signature of user B is provided for the data that consist of a card transfer offer response header 12016, which is header information indicating that the message is the card transfer offer response 7504 and describing the data structure; an acceptance number 12017; a transfer offer number 12018; a card ID 12019; an issued time 12020, which indicates the date on which the card transfer offer

response 7504 was issued; and a user public key certificate 12021. In this fashion, the card transfer offer response 7504 is provided.

[1874] The user public key certificate 12021 is a public key certificate for user B. To provide this certificate 12021, the digital signature of the service provider is provided for the data that consist of a user public key certificate header 12022; a user public key 12023 for user B; a public key certificate ID 12024, which is ID information for the public key certificate; a certificate validity term 12025; a service provider ID 12026; and a certificate issued time 12027.

[1875] The acceptance number 12017 is arbitrarily generated, by the mobile user terminal of user B, as a number that uniquely represents the payment card transfer processing. With this number, the mobile user terminal of user A is notified as to whether user B has accepted the card transfer offer 7501. When user B does not accept the card transfer offer 7501, a value of 0 is set as the acceptance number 12017. When user B accepts the card transfer offer 7501, a value other than 0 is set.

[1876] Upon receiving the card transfer offer response 7504, the mobile user terminal of user A displays, on the LCD, the contents of the card transfer offer response 7504 (display the transfer offer response; 7505). When the card transfer offer 7501 is accepted (acceptance number 12017 \neq 0), the mobile user terminal of user A examines the digital signature of the service provider of the user public key certificate 12021 and the validity term. The mobile user terminal generates a card transfer certificate 7506, which is a message that corresponds to a transfer certificate for an electronic payment card to user B, and transmits it to the mobile user terminal of user B.

[1877] As is shown in Fig. 121A, the digital signature of the electronic payment and the digital signature of user A are provided for the data that consist of a card transfer certificate header 12100, which is header information indicating that the message is the card transfer certificate 7506 and describing the data structure; a presentation card 12101 for an electronic payment card to be transferred; a card status 12102; a total remaining value 12103; a transfer offer number 12104; an acceptance number 12105; a public key certificate ID 12106 for the user public key certificate of user B; a public key certificate ID 12107 for the user public key certificate of user A; a card ID 12108; and an issued time 12109, which indicates the date on which the card transfer certificate 7506 was issued. These data are closed and addressed to user B, thereby providing the card transfer certificate 7506.

[1878] Upon receiving the card transfer certificate 7506, the mobile user terminal of user B decrypts it and examines the digital signature of user A and the one accompanying the electronic payment card. Further, the mobile user terminal compares the card ID presented by the card transfer offer 7501 with the card ID 12108,

and compares the public key certificate IDs 12106 and 12107 with the public key certificates of users B and A to verify the contents of the card transfer certificate 7506. The mobile user terminal then generates a card transfer receipt 7507, which is a message indicating the electronic payment card has been received, and transmits the receipt 7507 to the mobile user terminal of user A.

[1879] As is shown in Fig. 121B, the digital signature of user B is provided for the data that consist of a card transfer receipt header 12115, which is header information indicating that the message is the card transfer receipt 7507 and describing the data structure; a card ID 12116; a transfer offer number 12117; an acceptance number 12118; a public key certificate ID 12119 for the user public key certificate of user A; a public key certificate ID 12120 for the user public key certificate of user B; and an issued time 12121, which indicates the date on which the card transfer receipt 7507 was issued. These data are closed and addressed to user A, thereby providing the card transfer receipt 7507.

[1880] Upon receiving the card transfer receipt 7507, the mobile user terminal of user A decrypts it, and examines the digital signature of user B. Further, the mobile user terminal compares the public key certificate IDs 12119 and 12120 with the public key certificates of users B and A to verify the contents of the card transfer receipt 7507. The mobile user terminal then erases the transferred electronic payment card from the card list 1713, and registers the card transfer receipt 12122 in use history 1715. At this time, addresses in the object data area at which the transfer offer number, the code information indicating the card transfer process, the issued time for the card transfer receipt 7507 and the card transfer receipt 12122 are stored are assigned to the request number 1840 in the use list 1715, the service code 1841, the use time 1842 and the use information address 1843.

[1881] The mobile user terminal of user A displays, on the LCD, a message indicating the completion of the transfer process (display the transfer process; 7508). The process at the mobile user terminal of user A (sender) is thereafter terminated.

[1882] After transmitting the card transfer receipt 7507, the mobile user terminal of user B displays the received card transfer certificate 12111 on the LCD. In addition, the mobile user terminal displays a dialogue message inquiring whether the transfer process with the service providing server (process for downloading the received electronic payment card from the service providing system) should be immediately performed (display the transfer certificate; 7509).

[1883] The dialogue message has two operating menus: "transfer process request" and "cancel." When "cancel" is selected, the transfer process performed with the service providing server is canceled, and in the process (data updating process) during which the service providing system updates the data in the mobile

user terminal, an electronic payment card that has been transferred is assigned to the mobile user terminal.

[1884] When user B selects "transfer process request" (transfer process request operation; 7510), based on the card transfer certificate 12111 the mobile user terminal generates a card transfer request 7511, which is a message requesting that the transfer process be performed with the service providing system, and transmits it to the service providing system via digital wireless telephone communication.

[1885] As is shown in Fig. 122A, the digital signature of user B is provided for the data that consists of a card transfer request header 12200, which is header information indicating that the message is the card transfer request 7511 and describing the data structure; a decrypted card transfer certificate 12201 (12111); the user ID 12202 of user B; and an issued time 12203, which indicates the date when the card transfer request 7511 was issued. These data are closed and addressed to the service provider, thereby providing the card transfer request 7511.

[1886] Upon receiving the card transfer request 7511, the user processor of user B of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the card transfer request 12204.

[1887] The service director processor, first refers to the user list 5200 and specifies the recipient (user B) and the sender (user A) of the transfer process by employing the public key certificate IDs 12106 and 12107 in the card transfer certificate 12201 that is included in the card transfer request 12204. The service director processor examines the digital signature of the user A and the digital signature accompanying the electronic payment card, which are provided for the card transfer certificate 12201, and verifies the validity of the card transfer certificate 12201. Following this, the service director processor erases the electronic payment card to be transferred from the card list 4611 of the user A that is stored in the user information server 902. Then, the service director processor changes the card signature private key and card signature public key pair and the card certificate for a new key pair and a card certificate, and also changes the card status and the total remaining value to the card status 12102 and to the total remaining value 12103 for the card transfer certificate 12201. The service director processor generates an electronic payment card received from user A, and enters it in the card list 4611 for the user B.

[1888] When the electronic payment card that is to be transferred has already been registered, the service director processor updates the registered card list 5402 holding the electronic payment card. Specifically, the user ID 5418, the user public key 5419, the registered card certificate address 5420, the micro-check list address 5421 and the former user information address

5422, all of which are in the registered card list 5402, are updated (to the information for user B). The old information (information for user A) is pointed to at the former user information address 5422 as former user information 5423..

[1889] The service director processor generates a payment card transfer message 12215, which includes an electronic payment card transferred from user A. The user processor of user B closes the message 12215 and addresses it to the user B, and transmits it as a payment card transfer message 7512 to the mobile user terminal of user B via digital wireless telephone communication.

[1890] As is shown in Fig. 122B, the digital signature of the service provider is provided for the data that consist of a payment card transfer header 12208, which is header information indicating that the message is the card transfer 7512 and describing the data structure; a transfer number 12209, which is an arbitrarily generated number that represents the transfer process in the service providing system; transfer information 12210; an acceptance number 12211; an electronic payment card 12212, which is transferred; a service provider ID 12213; and an issued time 12214, which indicates the date when the payment card transfer message 7512 was issued. These data are closed and addressed to the user B, thereby providing the card transfer message 7512.

[1891] The transfer information 12210 is information concerning the electronic payment card transfer process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1892] The mobile user terminal of user B decrypts the received payment card transfer message 7512 and examines the digital signature, registers the electronic payment card 12212 in the card list 1713, and displays the electronic payment card on the LCD (display the electronic payment card; 7513). The card transfer process is thereafter terminated.

[1893] An explanation will now be given for the contents of messages that are exchanged by the devices during the electronic payment card installation processing.

[1894] In Fig. 78 are shown procedures for the exchange of messages by the devices during the electronic payment card installation processing, and in Figs. 125A and 125B, and 125A and 125B are shown the contents of messages that are exchanged during the electronic payment installation processing.

[1895] First, when the user performs an electronic payment card installation operation 7800, the mobile user terminal generates an electronic payment card installation request 7801, and transmits it to the service providing system 110 via digital wireless telephone communication.

[1896] As is shown in Fig. 125A, the digital signature of the user is provided for the data that consists of an

electronic payment card installation request header 12500, which is header information indicating that the message is the electronic payment card installation request 7801 and describes the data structure; an installation card number 12501 and an installation number 12502, which are entered by a user; a request number 12503, which is an arbitrarily generated number that uniquely represents the electronic payment card installation process; a user ID 12504; and an issued time 12505, which indicates the date when the electronic payment card installation request 7801 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card installation request 7801.

[1897] Upon receiving the electronic payment card installation request 7801, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the electronic payment card installation request 12506.

[1898] First, the service director processor refers to the installation card list that is indicated by the installation card list address 5236 for the payment card issuer list 5204, and specifies a payment card issuer who issues a payment card that is represented by the installation number 12501. The service director processor generates a payment card installation request 12517, which is a message requesting that the payment card issuer issue a payment card using the installation card. The payment card issuer processor closes the request 12517 and addresses it to the payment card issuer, and transmits it as a payment card installation request 7802 to the payment card issuing system 108.

[1899] As is shown in Fig. 125B, the digital signature of the service provider is provided for the data that consist of a payment card installation request header 12510, which is header information indicating that the message is the payment card installation request 7802 and describing the data structure; an installation card number 12511; an installation number 12512; a request number 12513; a customer number 12514, which uniquely represents a user for the payment card issuer; a service provider ID 12515; and an issued time 12516, which indicates the date when the payment card installation request 7802 was issued. These data are closed and addressed to the payment card issuer, thereby providing the payment card installation request 7802.

[1900] Upon receiving the payment card installation request 7802, the payment card issuing system 108 decrypts it and examines the digital signature. The payment card issuing server 1200 compares the installation card number 12511 and the installation number 12512, which are included in the payment card installation request 7802, with the management information for the issued electronic payment card installation card that is stored in the payment card issuing information server

1202. The payment card issuing server 1200 then updates the data in the customer information server 1202 and the payment card issuing information server 1203. Furthermore, the payment card issuing server generates payment card data (12606) for a requested payment card, and transmits, to the service providing system, an electronic payment card installation commission 7803, which is a message requesting the installation of an electronic payment card that corresponds to the requested payment card.

[1901] As is shown in Fig. 126A, the digital signature of the payment card issuer is provided for the data that consists of an electronic payment card installation commission header 12600, which is header information indicating that the message is the electronic payment card installation commission 7803 and describing the data structure; a transaction number 12601, which is an arbitrarily generated number that uniquely represents the transaction with a user; payment card issuing information 12602; a request number 12603; card code 12604, which indicates the type of electronic payment card that is to be issued; a template code 12605, which indicates a template program for an electronic payment card to be issued; payment card data 12606; representative component information 12607; a payment card issuer ID 12608; and an issued time 12609, which indicates the date when the electronic payment card installation commission 7803 was issued. These data are closed and addressed to the service provider, thereby providing the electronic payment card installation commission 7803.

[1902] The payment card issuing information 12602 is information concerning the payment card issuing process performed by the payment card issuing system, and is accompanied by the digital signature of the payment card issuer.

[1903] The payment card data 12606 is payment card information issued by the payment card issuer, wherein the digital signature of the payment card issuer accompanies the data that consists of the card ID 12614, the payment card information 12615 and the card ID 12616.

[1904] The payment card issuer processor of the service providing system decrypts the received electronic payment card installation commission 7803 and examines the digital signature, and transmits the commission 7803 to the service director processor. In accordance with the electronic payment card installation commission 12610, the service director processor generates an electronic payment card to be issued to a user, using the same procedures as are used for the payment card purchase processing, and also generates an electronic payment card installation message 12615, which is a message directing that the electronic payment card be installed in the mobile user terminal. The user processor closes the electronic payment card installation message 12655 and addresses it to a user, and transmits it as an electronic payment card installation message 7804 to the mobile user terminal via digital wireless telephone communication.

[1905] As is shown in Fig. 126B, the digital signature of the service provider is provided for the data that consists of an electronic payment card installation header 12617, which is header information indicating that the message is the electronic payment card installation message 7804 and describing the data structure; a transaction number 12618; payment card issuing information 12619, which concerns the payment card issuing process performed by the payment card issuing system; payment card issuing information 12620, which concerns the payment card issuing process performed by the service providing system; a request number 12621; generated electronic payment card data 12622; a service provider ID 12623; and an issued time 12624, which indicates the date when the electronic payment card installation message 7804 was issued. These data are closed and addressed to the user, thereby providing the electronic payment card installation message 7804. The payment card issuing information 12619 and the payment card issuing information 12620 are accompanied by the digital signatures of the payment card issuer and the service provider.

[1906] The mobile user terminal decrypts the received electronic payment card installation message 7804 and examines the digital signature, registers, in the card list 1713, the electronic payment card included in the electronic payment card installation request 7804, and displays the installed electronic payment card on the LCD (display the electronic payment card; 7805).

[1907] An explanation will now be given for the contents of messages that are exchanged by devices in various processes for electronic telephone card service.

[1908] First, an explanation will be given for the contents of messages that are exchanged by devices during the telephone card purchase processing.

[1909] In Fig. 63 are shown the procedures for the exchange of messages by devices during the telephone card purchase processing. In Figs. 101A and 101B, 102A and 102B, 103A and 103B, 104A and 104B, and 105A and 105B are shown the contents of messages that are exchanged by devices during the telephone card purchase processing.

[1910] First, when a user performs a telephone card purchase order operation 6300, the mobile user terminal transmits a telephone card purchase order 6301 to the service providing system through digital wireless telephone communication.

[1911] As is shown in Fig. 101A, the digital signature of a user is provided for data that consists of a telephone card purchase order header 10100, which is header information identifying the message as the telephone card purchase order 6301 and describing the data structure; a response code 10101, which identifies the type of service requested by the user; a card order code 10102, which identifies an order code for a telephone card that is entered by the user; a number of telephone cards 10103 that the user has entered; a payment service code 10104, which identifies a credit

card designated by the user; a payment value 10105; a payment option code 10106, which identifies a payment option, such as the number of payments designated by the user; a request number 10107, which is an arbitrarily generated number that uniquely represents the telephone card purchase processing; a validity term 10108 for the telephone card purchase order 6301; a user ID 10109; and an issued time 10110, which is the date on which the telephone card purchase order 6301 was issued. These data are closed and addressed to the service provider, thereby providing the telephone card purchase order 6301. The service code 8901 identifies the purchase order of a telephone card to a telephone card issuer who is selected by the user.

[1912] Upon receiving the telephone card purchase order 6301, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. Then, the service manager processor generates a service director processor to form a process group that processes a telephone card order 10111. The service director processor refers to the telephone card issuer list 5205 and generates a telephone card purchase order 10126 for the telephone card issuer indicated by the service code 10101. The telephone card issuer processor closes the telephone card order and addresses it to the telephone card issuer, and transmits the resultant order as a telephone card purchase order 6302 to the telephone card issuing system 109.

[1913] As is shown in Fig. 101B, the digital signature of a service providing system is provided for data that consists of a telephone card purchase order header 10115, which is header information indicating that the message is the telephone card purchase order 6302 and describing the data structure; a card order code 10116; a number of cards 10117 that are purchased; a payment service code 10118; a payment value 10119; a payment option code 10120; a request number 10121; a customer number 10122, which uniquely represents a user for the telephone card issuer; a validity term 10123 for the telephone card purchase order 6302; a service provider ID 10124; and an issued time 10125, which is the date on which the telephone card purchase order 6302 was issued. These data are closed and addressed to the telephone card issuer, thereby providing the telephone card purchase order 6302.

[1914] When there was a previous transaction to which the user and the telephone card issuer were parties, a customer number that is registered in the customer table of the telephone card issuer is established as the customer number 10122. When there was no previous transaction, the service director processor generates for the telephone card issuer a number that uniquely represents the user, establishes it as the customer number 10122, and registers that number in the customer table. The customer table is designated by using the customer table address 5244 of the telephone card issuer list 5205.

[1915] Upon receiving the telephone card purchase order 6302, the telephone card issuing system 109 decrypts it and examines the digital signature. The telephone card issuing server 1300 updates the data in the customer information server 1301, the telephone card issuing information server 1302 and the telephone card information server 1303, generates telephone card data (10219) for the ordered telephone card, and transmits, to the service providing system, an electronic telephone card issuing commission 6303, which constitutes a message requesting the process for issuing an electronic telephone card that corresponds to the telephone card and the process for settling the price of the telephone card.

[1916] As is shown in Fig. 102A, the digital signature of a telephone card issuer is provided for data that consists of an electronic telephone card issuing commission header 10200, which is header information identifying the message as the electronic telephone card issuing commission 6303 and describing the data structure; a transaction number 10201, which is an arbitrarily generated number that uniquely identifies a transaction to which a user is a party; a sales value 10202, which conveys the price of a telephone card; a clearing option 10203, which indicates which clearing procedures apply; a request number 10204; a telephone card code 10205, which identifies the type of electronic telephone card that is to be issued; a template code 10206, which identifies a template program to be used for an electronic telephone card that is to be issued; a number of telephone cards 10207, which indicates how many telephone cards are to be issued; telephone card data 10208; representative component information 10209; a telephone card issuer ID 10210; and an issued time 10211, which is the date on which the electronic telephone card issuing commission 6303 was issued. These data are closed and addressed to the service provider, thereby providing the electronic telephone card issuing commission 6303.

[1917] The clearing option 10203 is information by which the telephone card issuing system designates, to the service providing system, the procedures to be used for clearing the price of a telephone card. The clearing process is roughly divided into a spontaneous clearing process for issuing an electronic telephone card to a user after the price of the telephone card has been cleared, and a delayed clearing process for clearing the price of a telephone card after an electronic telephone card has been issued. The clearing option 10203 is used to designate either clearing process.

[1918] In the delayed clearing process, since an electronic telephone card is issued to a user before the clearing process is performed, the user does not have to wait.

[1919] For example, based on a purchase history maintained for customers, the telephone card issuer can designate the delayed clearing process for a customer with whom it has had dealings and who is known

to be trustworthy, and can designate the spontaneous clearing for a customer with whom it has had no previous dealings.

[1920] The telephone card data 10208 is telephone card information issued by the telephone card issuer. A number of telephone card information items equivalent to the number of telephone cards 10207 are established as the telephone card data 10208. For one telephone card, the digital signature of a telephone card issuer is provided for data that consist of a card ID 10216, card information 10217 and a telephone card issuer ID 10218, and the telephone card information is thereby provided. The telephone card information 10217 is ASCII information describing the contents of a telephone card. For the telephone card information 10217, the title of a telephone card, the face value of the telephone card that is issued, the usage condition, an issuer, and whether it can be transferred, are described using a form whereby tag information representing information types is additionally provided.

[1921] The representative component information 10209 is information that is established as the representative component information 2132 for an electronic telephone card to be generated. Therefore, the representative component information 10209 may not be set for use.

[1922] The telephone card issuer processor of the service providing system receives the electronic telephone card issuing commission 6303, decrypts it and examines the digital signature, and transmits it to the service director processor. The service director processor performs the electronic telephone card issuing process and the telephone card price clearing process in accordance with the clearing procedures designated by using the clearing option 10203.

[1923] In Fig. 63 is shown the spontaneous clearing process. The delayed clearing process will be described later.

[1924] For the spontaneous clearing, the service director processor generates a clearing request 10324, which is a message requesting the clearing of the price of a telephone card. The transaction processor processor closes the clearing request 10324 and addresses it to the transaction processor, and then transmits it as a clearing request 6304 to the transaction processing system 106.

[1925] As is shown in Fig. 103B, the digital signature of a service provider is provided for data that consists of a clearing request header 10314, which is header information indicating that the message is the clearing request 6304 and describing the data structure; a user clearing account 10315, which includes a credit card that corresponds to the payment service code designated by the user; a telephone card issuer clearing account 10316, which designates the clearing account of a telephone card issuer; a payment value 10317; a payment option code 10318; a request number 10319, which is issued by the mobile user terminal 100; a trans-

action number 10320, which is issued by the telephone card issuing system; a validity term 10321, which presents the period during which the clearing request 6304 is effective; a service provider ID 10322; and an issued time 10323, which indicates the date on which the clearing request 6304 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 6304.

[1926] The transaction processing system 106 receives the clearing request 6304, decrypts it and examines the digital Signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 6305, and transmits it to the service providing system 110.

[1927] As is shown in Fig. 104A, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 10400, which is header information indicating that the message is the clearing completion notification 6305 and describing the data structure; a clearing number 10401, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 10402; a telephone card issuer clearing account 10403; a payment value 10404; a payment option code 10405; a request number 10406; a transaction number 10407; clearing information 10408 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 10409 for a telephone card issuer that is accompanied by the digital signature of the transaction processor; clearing information 10410 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 10411; and an issued time 10412, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 6305.

[1928] Upon receiving the clearing completion notification 6305, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 10413 to the service director processor. Upon receiving the clearing completion notification 10413, the service director processor generates a clearing completion notification 10430 for the telephone card issuer. The telephone card issuer processor closes the clearing completion notification 10430, and transmits it to the telephone card issuing system 109 as a clearing completion notification 6306 for the telephone card issuer.

[1929] As is shown in Fig. 104B, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 10417, which is header information indicating that the message is the clearing completion notification 6306 and describing the data structure; a clearing number 10418; a customer number 10419; a telephone card issuer ID 10420; a

payment service code 10421; a payment value 10422; a payment option code 10423; a request number 10424; a transaction number 10425; clearing information 10426 for a telephone card issuer that is accompanied by the digital signature of the transaction processor; a transaction processor ID 10427; a service provider ID 10428; and an issued time 10429, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the telephone card issuer, thereby providing the clearing completion notification 6306.

[1930] Upon receiving the clearing completion notification 6306, the telephone card issuing system decrypts it and examines the digital signature, and generates a receipt 6307 and transmits it to the service providing system.

[1931] As is shown in Fig. 105A, the digital signature of a telephone card issuer is provided for data that consists of a receipt header 10500, which is header information indicating that the message is the receipt 6307 and describing the data structure; a customer number 10501; telephone card issuing information 10502; a payment service code 10503; a payment value 10504; a payment option code 10505; a request number 10506; a transaction number 10507; clearing information 10508; a transaction processor ID 10509; a telephone card issuer ID 10510; and an issued time 10511, which indicates the date on which the receipt 6307 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 6307. The telephone card issuing information 10502 is information concerning the telephone card issuing process performed by the telephone card issuing system, and is accompanied by the digital signature of the telephone card issuer.

[1932] Upon receiving the receipt 6307, the telephone card issuer processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 10512 to the service director processor. The service director processor employs the receipt 10512 to generate a receipt 10523 for a user.

[1933] In addition, the service director processor generates a clearing completion notification 10430 for the telephone card issuing system, generates an electronic telephone card to be issued to the user, and further generates an electronic telephone card issuing message 10227 that includes the electronic telephone card that is generated.

[1934] The user processor closes the electronic telephone card issuing message 10227 and the receipt 10523 while addressing them to the user, and transmits them as an electronic telephone card issuing message 6308 and a receipt 6309 to the mobile user terminal 100 via digital wireless communication.

[1935] As is shown in Fig. 102B, the digital signature of a service provider is provided for data that consist of an electronic telephone card issuing header 10220, which is header information indicating that the message

is the electronic telephone card issuing message 6308 and describing the data structure; a transaction number 10221; a request number 10222; the number of telephone cards 10223; electronic telephone card data 10224 that are generated; a service provider ID 10225; and an issued time 10226, which indicates the date on which the electronic telephone card issuing message 6308 was issued. These data are closed and addressed to the user, thereby providing the electronic telephone card issuing message 6308. The electronic telephone card data 10224 includes electronic telephone cards 10231 equivalent in number to the number of telephone cards 10223.

[1936] As is shown in Fig. 105B, the digital signature of a service provider is provided for data that consists of a receipt header 10516, which is header information indicating that the message is the receipt 6309 and describing the data structure; a user ID 10517; a receipt 10518 (10512) obtained by decryption; clearing information 10519 for a user that is accompanied by the digital signature of a transaction processor; telephone card issuing information 10520; a service provider ID 10521; and an issued time 10522, which indicates the date on which the receipt 6309 was issued. These data are closed and addressed to the user, thereby providing the receipt 6309. The telephone card issuing information 10520 is information for the electronic telephone card issuing process performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1937] Upon receiving the electronic telephone card issuing message 6308 and the receipt 6309, the mobile user terminal decrypts them and examines the digital signatures, enters in the telephone card list 1714 an electronic telephone card included in the electronic telephone card issuing message 6308, enters the receipt 10523 in the use list 1715, and displays the electronic telephone card on the LCD 303.

[1938] The generation of an electronic telephone card by the service director processor is performed as follows.

[1939] First, the service director processor refers to the electronic telephone card template list 5105 for the telephone card issuer that is stored in the telephone card issuer information server. Then, by using the electronic telephone card template program that is identified by the template code 10206 of the electronic telephone card issuing commission 6303, the service director processor generates a telephone card program for an electronic telephone card. Specifically, the telephone card program data 2113 for an electronic telephone card are generated using the transaction module and the representation module, which are described as being located at the transaction module address 5119, and the representation module address 5120 in the electronic telephone card template list 5105, and the representative component information 10209 in the electronic telephone card issuing commission 6303.

When the representative component information 10209 is not present in the electronic telephone card issuing commission 6303, the default representative component information located at the default representative component information address 5121 is employed as the information for an electronic telephone card.

[1940] Following this and based on the telephone card information included in the card information 10217, the service director processor generates the card status 2107 and the total remaining value 2108. Whether the card status 2107 can be transferred is designated, and the face value of the telephone card that is issued is set as the total remaining value 2107. The service director processor generates a new pair consisting of a card signature private key and a card signature public key, and further generates the telephone card program 2101 for an electronic telephone card by employing the card private key and the accounting machine public key that are registered in the electronic telephone card management information 5500.

[1941] Furthermore, the service director processor generates an electronic telephone card by employing the obtained card signature public key to generate the certificate 2103 for the electronic telephone card, and by employing the telephone card data 10219 in the electronic telephone card issuing commission 6303 to generate the presentation card 2102 for the electronic telephone card.

[1942] The procedures for the delayed clearing will now be described.

[1943] In Fig. 64 are shown the procedures for exchanging messages between the devices in the telephone card purchase process for the delayed clearing. The same process is performed as is used for the spontaneous clearing until the telephone card issuing system transmits the electronic telephone card issuing commission to the service providing system.

[1944] When the delayed clearing is designated by the clearing option 10203, the service director processor generates an electronic telephone card to be issued to the user, and also generates the electronic telephone card issuing message 10227, which includes the generated electronic telephone card, and a temporary receipt message 10310, which corresponds to a temporary receipt. The generation of the electronic telephone card is performed in the same manner as that used for the spontaneous clearing.

[1945] The user processor closes the electronic telephone card issuing message 10227 and the temporary receipt 9810 and addresses them to the user, and transmits these messages as an electronic telephone card issuing message 6404 and a temporary receipt 6405 to the mobile user terminal 100 via digital wireless telephone communication.

[1946] As is shown in Fig. 103A, the digital signature of a service provider is provided for data that consists of a temporary receipt header 10300, which is header information indicating that the message is the tempo-

rary receipt 6405 and describing the data structure; a user ID 10301; telephone card issuing information 10302; a payment service code 10303; a payment value 10304; a payment option code 10305; a request number 10306; a transaction number 10307; a service provider ID 10308; and an issued time 10309, which indicates the date on which the temporary receipt 6405 was issued. These data are closed and addressed to the user, thereby providing the temporary receipt 6405.

The telephone card issuing information 10302 is information concerning the electronic telephone card issuing process that is performed by the service providing system, and is accompanied by the digital signature of the service provider.

[1947] The data structure of the electronic telephone card issuing message 6404 is the same as that used for the electronic telephone card issuing message 6308.

[1948] Upon receiving the electronic telephone card issuing message 6404 and the temporary receipt 6405, the mobile user terminal decrypts them and examines the digital signatures, enters an electronic telephone card included in the electronic telephone card issuing message 6404 in the telephone card list 1714, enters the temporary receipt 10310 in the use list 1715, and displays the electronic payment card on the LCD 303.

[1949] Following this, the service director processor performs the clearing process for the price of the telephone card. First, the service director processor generates a clearing request 10324, which is a message requesting the performance of the clearing process for the price of the telephone card. The transaction processor closes the clearing request 10324 and addresses it to the transaction processor, and transmits it as a clearing request 6407 to the transaction processing system 106.

[1950] Upon receiving the clearing request 6407, the transaction processing system 106 decrypts it and examines the digital signature, and performs the clearing process. The transaction processing system 106 generates a clearing completion notification 6408 and transmits it to the service providing system 110.

[1951] Upon receiving the clearing completion notification 6408, the transaction processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 10413 to the service director processor. The service director processor employs the received clearing completion notification 10413 to generate a clearing completion notification 10430 for the telephone card issuer. And the telephone card issuer processor closes the clearing completion notification 10430 and transmits it to the telephone card issuing system 109 as a clearing completion notification 6409 for the telephone card issuer.

[1952] The telephone card issuing system decrypts the received clearing completion notification 6409 and examines the digital signature, and generates a receipt 6410 and transmits it to the service providing system.

[1953] The telephone card issuer processor of the service providing system decrypts the received receipt 6410 and examines the digital signature, and transmits a receipt 10512 to the service director processor. The service director processor employs the receipt 10512 to generate a receipt 10523 for a user.

[1954] The receipt 10523 that is generated is not immediately transmitted to the mobile user terminal 100 of the user. When the mobile user terminal has performed the data updating process, the user processor replaces the temporary receipt 10310 in the use list 1715 with the receipt 10523, and transmits the receipt 10523 as one part of the update data 6411 to the mobile user terminal 100.

[1955] The data structures of the clearing request 6407, the clearing completion notification 6408, the clearing completion notification 6409 and the receipt 6410 for the delayed clearing are the same as those provided for the clearing request 6304, the clearing completion notification 6305, the clearing completion notification 6306 and the receipt 6307 for the spontaneous clearing.

[1956] The delayed clearing process need not be performed immediately after the electronic telephone card is issued, and together with the other clearing processes, may be performed, for example, once a day.

[1957] An explanation will now be given for the contents of messages that are exchanged by the mobile user terminal 100 and the service providing system 110 during the telephone card registration processing.

[1958] In Fig. 65C are shown the procedures for exchanging messages between devices in the telephone card registration processing, and in Figs. 108A and 108B are shown the contents of messages that are exchanged by the devices in the telephone card registration processing.

[1959] First, when the user performs an electronic telephone card registration operation 6508, the mobile user terminal generates a telephone card registration request 6509 and transmits it to the service providing system via digital wireless telephone communication.

[1960] As is shown in Fig. 108A, the digital signature of a user is provided for data that consists of a telephone card registration request header 10800, which is header information indicating that the message is the telephone card registration request 6509 and describing the data structure; a card ID 10801 of a telephone card to be registered; a user ID 10802; and an issued time 10803, which indicates the date on which the telephone card registration request 6509 was issued. These data are closed and addressed to the service provider, thereby providing the telephone card registration request 6509.

[1961] The user processor of the service providing system decrypts the received telephone card registration request 6509 and examines the digital signature, and transmits the request 6509 to the service manager processor. The service manager processor generates a

service director processor to form a process group that processes a telephone card registration request 10804. The service director processor ascertains that the electronic telephone card indicated by the card ID 10801 is registered in the telephone card list 4612 for the user in the user information server 902, and registers that electronic telephone card in the registered card list 5502 for electronic telephone cards of the service director information server 901. At this time, the service director processor newly generates a card signature private key and a card signature public key pair. Further, the service director processor generates a registered card certificate using the card signature public key, and registers it in the registered card list 5502. The service director processor then generates a card certificate issuing message 10813 using the card signature private key and the registered card certificate that has been generated. The user processor closes the card certificate issuing message 10813 and addresses it to the user, and transmits it as a telephone card certificate issuing message 6510 to the mobile user terminal via digital wireless telephone communication.

[1962] As is shown in Fig. 108B, the digital signature of a service provider is provided for data that consists of a telephone card certificate issuing header 10808, which is header information indicating that the message is the telephone card certificate issuing message 6510 and describing the data structure; a card digital signature private key 10809; a registered card certificate 10810; a service provider ID 10811, and an issued time 10812, which indicates the date on which the telephone card certificate issuing message 6510 was issued. These data are closed and addressed to the user, thereby providing the telephone card certificate issuing message 6510.

[1963] The mobile user terminal 100 decrypts the received card certificate issuing message 6510 and examines the digital signature, replaces the card signature private key and the card certificate of an electronic telephone card with the card signature private key 10809 and the registered card certificate 10810, both of which are included in the telephone card certificate issuing message 6510, changes the registration state in the card status to the post-registration state, and displays on the LCD the electronic telephone card that has been registered (display a telephone card that is registered; 6511).

[1964] An explanation will now be given for the contents of messages that are exchanged by the service providing system 110 and the electronic telephone card accounting machine 800 (switching center 105) during the telephone card setup processing.

[1965] The telephone card setup processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the electronic telephone card accounting machine 800.

[1966] Therefore, for the telephone card setup process, the procedures for the exchange of messages by the service providing system and the electronic telephone card accounting machine 800, and the contents (data structures) of the messages to be exchanged are the same as those used for the above described data updating processing.

[1967] It should be noted, however, that the telephone card setup process is not performed each time the data updating process is performed, but when the telephone card list 4610 for the merchant stored in the merchant information server 903 is updated by the service director processor.

[1968] When the telephone card list 4610 is updated, the merchant processor includes updated data in the telephone card list 4610 for the compressed update data 8828 in the update data 5705, and transmits the resultant data as update data 5705 to the electronic telephone card accounting machine 800.

[1969] Upon receiving the update data 5705, the electronic telephone accounting machine decompresses the update data 8828, and updates the data in the RAM and on the hard disk. At this time, the telephone card list 3908 in the electronic telephone card accounting machine 800 is updated, and an electronic telephone card that is handled by the electronic telephone card accounting machine 800 is updated.

[1970] An explanation will now be given for the contents of messages that are exchanged by between the mobile user terminal 100 and the electronic telephone card accounting machine 800 (switching center 105) during the telephone card clearing processing.

[1971] In Fig. 70 are shown procedures for the exchange of messages by the mobile user terminal 100 and the electronic telephone card accounting machine 800 (switching center 105) during the telephone card clearing processing, and in Figs. 114A and 114B and Figs. 115A and 115B are shown the contents of messages that are exchanged by the mobile user terminal 100 and the electronic telephone card accounting machine 800 (switching center 105) during the telephone card clearing processing.

[1972] First, when a user displays an electronic telephone card used for communication and performs a calling operation 7000, the mobile user terminal employs a telephone card that is to be used for communication and an arbitrarily generated test pattern and produces a micro-check call request 7001, which is a message for requesting that a telephone number entered by a user be dialed by using the electronic telephone card. The mobile user terminal transmits the request 7001 to the switching center 105 via infrared communication.

[1973] As is shown in Fig. 114A, the micro-check call request 7001 consists of a micro-check call request header 11400, which is header information indicating that the message is the micro-check call request 7001 and describes the data structure; a service code 11401,

which identifies the request for communication using an electronic telephone card; a request number 11402, which is an arbitrarily generated number that uniquely represents the telephone card clearing process; an telephone number 11403 that is a telephone number entered by the user; a presentation card 11403 for presenting an electronic telephone card to be used for the communication; a card certificate 11405; a current card status 11406 for an electronic telephone card to be used for the communication; a total remaining value 11407; a card ID 11408; an issued time 11409, which indicates the date on which the micro-check call request 7001 was issued; and an accounting machine test pattern 11411, which is an arbitrarily generated test pattern. The digital signature is provided, using the card signature private key of an electronic telephone card, for the card status 11406, the total remaining value 11407, the card ID 11408 and the issued time 11409. The accounting machine test pattern 11411 is encrypted using the accounting machine public key.

[1974] The presentation card 11404, the card certificate 11405, the card status 11406, the total remaining value 11407, the card ID 11408 and the issued date 11409 specify the contents of the electronic telephone card for the electronic telephone card accounting machine 800, and the accounting machine test pattern 11411 is a test pattern for authorizing the electronic telephone card accounting machine 800.

[1975] Upon receiving the micro-check call request 7001 at the switching center 105, first, the electronic telephone card accounting machine 800 refers to the telephone card list 3908 and activates a telephone card clearing module that corresponds to the card code (included in a presentation card) for the electronic telephone card that is presented. Then, the electronic telephone card accounting machine 800 examines the validity of the contents of the micro-check call request 7001, generates a micro-check call response 7002, which charges a communication fee V ($V < 0$) for a predetermined communication T ($T > 0$), and transmits it to the mobile user terminal via digital wireless telephone communication. When the electronic telephone card that is presented is not registered in the telephone card list 3908, the micro-check call response 3908 is transmitted, which indicates that the pertinent electronic telephone card is not available.

[1976] In the verification processing for determining the validity of the micro-check call request 7001, first, the electronic telephone card accounting machine 800 employs the fact that the card certificate 11405 is a registered card certificate, and examines the card status 11406 and the total remaining value 11407 to determine whether the electronic telephone card is valid and can be used as a telephone card for the payment of the communication charge. Then, the electronic telephone card accounting machine 800 examines the presentation card 11404, the digital signature of the service provider that is provided for the card certificate 11405, and

the validity term. Further, the merchant terminal employs the card signature public key of the card certificate 11405 to examine the digital signature of the electronic telephone card that is provided for the card status 11406, the total remaining value 11407, the card ID 11408 and the issued time 11409. In this fashion, the validity of the micro-check call request 7001 is verified.

[1977] In the generation of the micro-check call response 7002, the electronic telephone card accounting machine 800 decrypts the accounting machine test pattern 11411 using the accounting machine private key, and employs the card public key to encrypt the card test pattern 11411 that is arbitrarily generated.

[1978] As is shown in Fig. 114B, the digital signature of a communication service provider is provided for the data that consists of a micro-check call response header 11413, which is header information indicating that the message is the micro-check call response 7002 and describing the data structure; a transaction number 11414; a response message 11415; a request number 11416; a card ID 11417; an instruction code 11418; an amount of charge 11419, which indicates the communication fee V for the communication time T; an accounting machine test pattern 11420, which is decrypted; a card test pattern 11421, which is an arbitrarily generated test pattern; an accounting machine ID 11423; a communication service provider ID 11424; and an issued time 11425, which indicates the date on which the micro-check call response 7002 was issued. In this fashion, the micro-check call response 7002 is provided. The card test pattern 11421 is encrypted using the card public key.

[1979] The transaction number 11414 is a number that is arbitrarily generated, by the electronic telephone card accounting machine 800, and that uniquely represents the telephone card clearing process. When, as a result of the examination of the micro-check call request 7001, the telephone card clearing process can not be performed (when an electronic telephone card is one that can not be handled by the pertinent electronic telephone card accounting machine 800), a value of 0 is set. When the telephone card clearing process can be performed, a value other than 0 is set.

[1980] The response message 11415 is text information constituting the message transmitted by the communication service provider to the user. When the electronic telephone card accounting machine 800 can not handle an electronic telephone card that has been presented (transaction number = 0), data to that effect is included in the response message. The response message is prepared optionally, and may not be prepared.

[1981] The instruction code 11418 is command code information for an electronic telephone card, and is used when a value equivalent to the amount of charge 11419 is subtracted from the total remaining value held by the electronic telephone card. The instruction code is varied by combining the electronic telephone card transaction module and the telephone card clearing

module.

[1982] When the mobile user terminal receives the micro-check call response 7002, first, for verification of to verify the electronic telephone card accounting machine 800, it compares the accounting machine test pattern 11411 with the accounting machine test pattern 11420 included in the micro-check call response 7002 in order to verify the electronic telephone card accounting machine 800. The mobile user terminal subtracts the amount of sales 11419 from the total remaining value held by the electronic telephone card in accordance with the instruction code 11418. Then, the mobile user terminal decrypts the card test pattern using the card private key, and generates a telephone micro-check message 7003, which corresponds to a check that has as its face value the amount of the charge. The check is transmitted via digital wireless telephone communication to the electronic telephone card accounting machine 800 (switching center 105). Further, the mobile user terminal displays, on the LCD, a message indicating a call is on process (display a call on process; 6704)

[1983] As is shown in Fig. 115A, the digital signature using the card signature private key and the digital signature of a user are provided for the data that consists of a telephone micro-check header 11500, which is header information indicating that the message is the telephone micro-check 7003 and describing the data structure; a micro-check issuing number 11501, which indicates the order of the telephone card clearing process; a card test pattern 11502, which is decrypted; an amount of payment 11503, which indicates the obtained value that is subtracted from the total remaining value; a card status 11504; a total remaining value 11505 available after the subtraction; an accounting machine ID 11506; a communication service provider ID 11507; a request number 11508; a transaction number 11509; a card code 11510; a card ID 11511; and an issued time 11512, which indicates the date on which the telephone micro-check 7003 was issued. In this fashion, the telephone micro-check 7003 is provided.

[1984] Upon receiving the telephone micro-check 7003 at the switching center 105, first, the electronic telephone card accounting machine 800 authorizes the electronic telephone card by comparing the card test pattern 11421 with the card test pattern 11502 that is included in the telephone micro-check 7003, and examines the validity of the contents of the telephone micro-check 7003. In the verification process for the validity of the telephone micro-check 7003, the electronic telephone accounting machine 800 determines whether the amount of payment 11503 represented by the telephone micro-check 7003 is equal to the value of the charge. Also, the electronic telephone card accounting machine 800 determines whether the value obtained by subtracting the total remaining value 11505 from the total remaining value 11407, which represents the micro-check call request, is equal to the amount of payment 11503 represented by the telephone micro-check.

Finally, the electronic telephone card accounting machine 800 examines the digital signature of the electronic telephone card accompanying the telephone micro-check 7003.

[1985] The switch 801 transmits, to the telephone terminal 115, a call arrival request 7005, which is a message for calling the telephone terminal 115 that corresponds to the telephone number 11403. Upon receiving the call arrival request 7005, the telephone terminal 115 outputs a call tone to notify the owner (call receiver) of the telephone terminal 115 that a call has arrived (display the arrival of a call; 7006). When the recipient raises the handset (communication operation 7007), the telephone terminal 115 transmits, to the switch 801, a call response 7008, which is a message to permit the call.

[1986] When the switch 801 receives the call response 7008, the electronic telephone card accounting machine 800 generates a receipt message 7009 that corresponds to a receipt for the telephone micro-check 7003 that is paid, and transmits the message to the mobile user terminal via digital wireless telephone communication. The switch 801 connects the lines of the mobile user terminal 100 and the telephone terminal 115, so that the user can communicate with the call recipient.

[1987] As is shown in Fig. 115B, the digital signature of a merchant is provided for the data that consists of a receipt header 11514, which is header information indicating that the message is the receipt 7009 and describing the data structure; provided service information 11515; a card ID 11516; a total receipt value 11517, which reflects the same value as the amount of payment 11503 remitted by the telephone micro-check that is received; a request number 11518; a transaction number 11519; a telephone micro-check issuing number 11520; an accounting machine ID 11521; a communication service provider ID 11522; and an issued time 11523, which indicates the date on which the receipt 7009 was issued. In this fashion, the receipt 7009 is provided.

[1988] The provided service information 11515 is text information that represents the contents of the communication service provided through the telephone card clearing process, and corresponds to the specifications or the statement of accounts for the services that are provided.

[1989] Upon receiving the receipt 7009, the mobile user terminal verifies that the total receipt value 11517 is equal to the amount of payment 11503 remitted using the telephone micro-check, registers the receipt 7009 as usage information in the usage list 1715, and changes the display on the LCD to a display indicating the connection state (the telephone number used for communication, the elapsed communication time and the total remaining value of an electronic telephone card) (display the connection state; 7010).

[1990] When the mobile user terminal 100 does not

receive the receipt 7009 after it has transmitted the telephone micro-check 7003, for example, when the user presses the end switch 306 while the ringing is in progress and cancels the call before the receipt 7009 is received, the mobile user terminal 100 adds the amount of sales 11419 to the total remaining value of the electronic telephone card, and returns the value to what it was before the subtraction was performed.

[1991] When the communication time exceeds T, instead of the telephone micro-check 7003 having the face value V, the electronic telephone accounting machine transmits a communication charge message 7011, which is a charge requiring the submission of a telephone micro-check having a face value that equals a communication fee 2V charged for a communication time 2T, to the mobile user terminal via digital wireless telephone communication.

[1992] As is shown in Fig. 115C, the digital signature of a communication service provider is provided for the data that consists of a communication charge response header 11524, which is header information indicating that the message is the communication charge 7011 and describing the data structure; a transaction number 11515; a request number 11526; a card ID 11527; an instruction code 11528; an amount of charge 11529, which accesses an additional charge value V; an accounting machine ID 11530; a communication service provider ID 11531; and an issued time 11532, which indicates the date on which the communication charge 7011 was issued. In this fashion, the communication charge 7011 is provided. The transaction number 11525 is the same as the transaction number 11414 provided for the micro-check call response 7002, the transaction number 11509 for the telephone micro-check 7003, and the transaction number 11519 for the receipt 7009.

[1993] Upon receiving the communication charge 7011, the mobile user terminal subtracts the amount of charge 11529 (the additional charge value V) from the total remaining value of the electronic telephone card. Instead of the telephone micro-check 7003, the mobile user terminal generates a telephone micro-check 7012, which has a face value of 2V that corresponds to the total value subtracted from the total remaining value, and transmits it to the electronic telephone accounting machine 800 (switching center 105) via digital wireless telephone communication.

[1994] As is shown in Fig. 115A, the data structure of the telephone micro-check 7012 is the same as that of the telephone micro-check 7003. The amount of payment 11503 remitted by the telephone micro-check 7012 is 2V, which corresponds to the total value subtracted from the total remaining value, and the total remaining value 11505 is the total remaining value after the amount of charge 11529 has been subtracted.

[1995] The same numbers as are used for the telephone micro-check 7003 are also employed as the micro-check issuing number 11501, the request number

11508 and the transaction number 11509 in the telephone micro-check 7012, which identify the telephone micro-check that is issued as the replacement for the telephone micro-check 7003.

[1996] Upon receiving the telephone micro-check 7012, the electronic telephone card accounting machine verifies the validity of the telephone micro-check 7012, and generates a receipt message 7013 that corresponds to a receipt for the telephone micro-check 7012 that has been issued and transmits it to the mobile user terminal via the digital wireless telephone terminal.

[1997] During the process of examining the validity of the telephone micro-check 7012, first, the electronic telephone card accounting machine 800 ascertains that the amount of payment 11503 reflected by the telephone micro-check 7012 is equal to the total amount charged, and ascertains that the result obtained by subtracting the total remaining value 11505, indicated by the telephone micro-check 7012, from the amount of stored value 11407, indicated by the macro check call request, is equal to the total amount of payment 11503 reflected by the telephone micro-check. Then, the accounting machine 800 examines the digital signature that is provided for the telephone micro-check 7012 using the electronic telephone card.

[1998] As is shown in Fig. 115A, the data structure of the receipt 7013 is the same as that used for the receipt 7009. The total receipt value 11517 of the receipt 7013 is equal to the amount of payment 11503 reflected by the telephone micro-check 7012.

[1999] Upon receiving the receipt 7013, the mobile user terminal verifies that the total receipt value 11517 is equal to the amount of payment 11503 reflected by the telephone micro-check 7012, registers the receipt 7013, instead of the receipt 7009, as usage information in the usage list 1715, and updates the total remaining amount of the electronic telephone card that is displayed on the LCD (display the accounts; 7014).

[2000] When the mobile user terminal 100 does not receive the receipt 7013 after it has transmitted the telephone micro-check 7012, such as when, for example, the communication is terminated before the receipt 7013 is received, the mobile user terminal 100 adds the amount of charge 11529 to the total remaining value of the electronic telephone card, and returns the value to what it was before the amount of charge 11529 was subtracted.

[2001] Each time the communication time exceeds NT (T is a natural number), instead of the telephone micro-check having the face value NV, the electronic telephone accounting machine 800 transmits a communication charge message 7015, which includes a charge for a telephone micro-check having as a face value a communication fee $(N+1)V$ that is assessed for a communication time $(N+1)T$, to the mobile user terminal via digital wireless telephone communication. As is shown in Fig. 115C, the data structure of the communication

charge 7015 is the same as that used for the communication charge 7011.

[2002] The mobile user terminal further subtracts the amount of charge 11529 (additional communication charge value V) from the total remaining value of the electronic telephone card, generates a telephone micro-check 7016 having a face value of $(N+1)V$, which corresponds to the total value subtracted from the total remaining value, and transmits it to the electronic telephone card accounting machine 800 (switching center 105) via digital wireless telephone communication.

[2003] As is shown in Fig. 115A, the data structure of the telephone micro-check 7016 is the same as that used for the telephone micro-check 7003 or 7012. The amount of payment 11503 reflected by the telephone micro-check 7016 is $(N+1)V$, which corresponds to the total value subtracted from the total remaining value, and the total remaining value 11505 is that which is available after the amount of charge 11529 has been subtracted.

[2004] Upon receiving the telephone micro-check 7016, the electronic telephone card accounting machine 800 examines the validity of the telephone micro-check 7016, and generates a receipt message 7017 that corresponds to a receipt for the telephone micro-check 7016 that has been paid and transmits it to the mobile user terminal via digital wireless telephone communication.

[2005] During the process of examining the validity of the telephone micro-check 7016, first, the electronic telephone card accounting machine 800 ascertains that the amount of payment 11503 reflected by the telephone micro-check 7016 is equal to the total amount of the charge, and ascertains that the result obtained by subtracting the total remaining value 11505, indicated by the telephone micro-check, from the total remaining value 11407, indicated by the macro check call request, is equal to the total amount of payment 11503 reflected by the telephone micro-check. Then, the accounting machine 800 uses the electronic telephone card to examine the digital signature that is provided for the telephone micro-check 7016.

[2006] As is shown in Fig. 115B, the data structure of the receipt 7017 is the same as that used for the receipt 7013. The total receipt value 11517 of the receipt 7017 is equal to the amount of payment 11503 of the telephone micro-check 7016.

[2007] Upon receiving the receipt 7017, the mobile user terminal verifies that the total receipt value 11517 is equal to the amount of payment 11503 reflected by the telephone micro-check 7016, registers the receipt 7017, instead of the receipt having type same request number (the previously registered receipt), as usage information in the usage list 1715, and updates the total remaining amount of the electronic telephone card that is displayed on the LCD (display the accounts; 7018).

[2008] When the mobile user terminal 100 does not receive the receipt 7017 after it has transmitted the tel-

ephone micro-check 7016, such as when, for example, the communication is terminated before the receipt 7017 is received, the mobile user terminal 100 adds the amount of charge 11529 transmitted in the communication charge message 7015 to the total remaining value of the electronic telephone card, and returns the value to what it was before the amount of charge 11529 was subtracted.

[2009] When a communication session using the electronic telephone card is terminated, the mobile user terminal 100 increments the micro-check issue number of the electronic telephone card.

[2010] At the termination of a communication session, the electronic telephone card accounting machine 800 registers, in the transaction list 3909, the receipt that has been transmitted to the mobile user terminal and the corresponding telephone micro-check as history information for the telephone card clearing process.

[2011] The contents of the call arrival request 7005 and the call response 7008, which are messages exchanged by the switching center 105 and the telephone terminal 115, depend on the protocol for the line connection established between the switching center 105 and the telephone terminal 115.

[2012] An explanation will now be given for the contents of messages that are exchanged by the devices during the telephone card reference processing.

[2013] In Fig. 73 are shown procedures for the exchange of messages by the devices during the telephone card reference processing, and in Figs. 88A to 88D and Fig. 116B are shown the contents of messages that are exchanged during the telephone card reference processing.

[2014] The telephone card reference processing is not performed in accordance with a special processing sequence, but is performed in the data updating process during which the service providing system updates the data in the electronic telephone card accounting machine 800.

[2015] Therefore, for the telephone card reference process, the procedures for the exchange of messages by the electronic telephone card accounting machine 800 and the service providing system, and the contents (data structures) of the messages to be exchanged are the same as those employed for the above described data updating processing.

[2016] Compressed upload data 8818 in the upload data 5704 include a telephone micro-check that is newly registered in the transaction list 3909 during the telephone card clearing process conducted during the period extending from the previous performance of the data updating process to the current performance of the data updating process.

[2017] During the data updating processing, the merchant processor transmits, to the service manager processor, a message requesting the reference process be performed for the telephone micro-check that is uploaded from the electronic telephone card accounting

machine 800. The service manager processor generates a service director processor to form a process group for examining the validity of the telephone micro-check.

[2018] First, the service director processor determines whether the accounting machine ID 11505 and the communication service provider ID 11506 in the telephone micro-check match the accounting machine ID 5215 of the communication service provider and the communication service provider ID 5214. Then, the service director processor examines the registered card list 5502 in the service director information server 901 to verify that the electronic telephone card for which the telephone micro-check was issued is registered. The service director processor employs the user public key 5519 to examine the digital signature of the user that accompanies the telephone micro-check, and employs the registered card certificate to examine the digital signature for the telephone card that accompanies the telephone micro-check. In addition, the service director processor employs the telephone micro-check issuing number when examining the matching of the amount of payment with the total remaining value, and transmits the result of the examination to the merchant processor. As a result, the telephone micro-check that is ascertained to be valid is registered in the telephone micro-check list.

[2019] When an error occurs in the process for verifying the validity of the telephone micro-check, the service director processor transmits a message indicating that an error occurred in the management system 908.

[2020] Upon receiving the update data 5705, the electronic telephone card accounting machine 800 decompresses the update data 8828 and updates the data in the RAM and on the hard disk.

[2021] If the firm represented by the communication service provider differs from that represented by the telephone card issuer, and a payment for the communication service provider who handles the telephone card is made by the telephone card issuer, or if the usage of the telephone card is periodically reported to the telephone card issuer in accordance with the terms of a contract, in accordance with the telephone micro-check that is newly registered in the telephone micro-check list, the service director processor generates weekly, for example, a usage condition notification 11626, which is a message for notifying the telephone card issuer of the telephone card usage condition. The telephone card issuer processor closes the notification 11626 and addresses it to the telephone card issuer, and transmits it as a usage report 7300 to the telephone card issuing system 109.

[2022] As is shown in Fig. 116C, the digital signature of a service provider is provided for the data that consists of a usage report header 11620, which is header information indicating that the message is the usage report 7300 and describing the data structure; a card ID and payment value list 11621 of telephone cards that are employed; the communication service provider

name 11622 and the communication service provider ID 11623 of a communication service provider that handles the telephone card; a service provider ID 11624; and an issued time 11625, which indicates the date on which the usage report 7300 was issued. These data are closed and addressed to the telephone card issuer, thereby providing the usage report 7300.

[2023] Upon receiving the usage report 7300, the telephone card issuing system 109 decrypts it and examines the digital signature, and performs such processing as making a payment to the merchant.

[2024] An explanation will now be given for the contents of messages that are exchanged by the devices during the telephone card transfer processing.

[2025] In Fig. 76 are shown procedures for the exchange of messages by the devices during the telephone card transfer processing, and in Figs. 120A and 120B, 121A and 121B, and 122A and 122C are shown the contents of messages that are exchanged during the telephone card transfer processing.

[2026] The telephone card transfer process can be performed when the card status 2107 of the electronic telephone card indicates the transfer enabled state, which is designated by the telephone card issuer when issuing a telephone card.

[2027] In Fig. 76 is shown a case where user A transfers an electronic telephone card to user B. The procedures for the exchange of messages by the devices belonging to users A and B are the same for infrared communication as they are for digital wireless communication. The data structures of messages are also the same.

[2028] In Fig. 76, first, when user A performs a telephone card transfer process 7600, the mobile user terminal of user A transmits a telephone card transfer offer 7601, which is a message offering to transfer an electronic telephone card, to the mobile user terminal of user B. When at this time the mobile user terminals of user A and user B are connected, communication between user A and user B is performed via digital wireless telephone. When the mobile user terminals are not connected, infrared communication is employed.

[2029] As is shown in Fig. 120A, the digital signature of user A is provided for the data consisting of a card transfer offer header 12000, which is header information indicating that the message is the card transfer offer 7601 and describing the data structure; a transfer offer number 12001, which is an arbitrarily generated number that uniquely represents the telephone card transfer process; a presented card 12002 and a card certificate 12003 for an electronic telephone card to be transferred; a card status 12004; a total remaining value 12005; a card ID 12006; an issued time 12007, which indicates the date on which the card transfer offer 7601 was issued; and a user public key certificate 12009. In this fashion, the card transfer offer 7501 is provided. The digital signature of the electronic telephone card is provided, using the card signature private key, for the

card status 12004, the variable card information 12005, the card ID 12006 and the issued time 12007.

[2030] The digital signature of the service provider is provided for the data that consist of a user public key header 12010; the user public key 12011 of user A; a public key certificate ID 12012, which is ID information for the public key certificate; a certificate validity term 12013; a service provider ID 12014; and a certificate issued time 12015. In this fashion, the user public key certificate 12009 is provided.

[2031] Upon receiving the card transfer offer 7601, the mobile user terminal of user B examines the presented card 12002, the card certified 12003, and the digital signature of the service provider and the validity term of the public key certificate 12009. Then, the mobile user terminal examines the digital signature of the electronic telephone card that is provided for the card status 12004, the total remaining value 12005, the card ID 12006 and the issued time 12007, and the digital signature of user A accompanying the card transfer offer 7601, and verifies the contents of the card transfer offer 7501. In accordance with the presented card 12002, the card status 12004 and the total remaining value 12005, the mobile user terminal then displays, on the LCD, the contents of the electronic telephone card that is to be transferred (display the transfer offer; 7602).

[2032] When user B performs a transfer offer acceptance operation 7603, the mobile user terminal of user B transmits, to the mobile user terminal of user A, a card transfer offer response 7604, which is a response message for the card transfer offer 7601.

[2033] As is shown in Fig. 120B, the digital signature of user B is provided for the data that consist of a card transfer offer response header 12016, which is header information indicating that the message is the card transfer offer response 7604 and describing the data structure; an acceptance number 12017; a transfer offer number 12018; a card ID 12019; an issued time 12020, which indicates the date on which the card transfer offer response 7604 was issued; and a user public key certificate 12021. In this fashion, the card transfer offer response 7604 is provided.

[2034] The user public key certificate 12021 is a public key certificate for user B. To provide this certificate 12021, the digital signature of the service provider is provided for the data that consist of a user public key certificate header 12022; a user public key 12023 for user B; a public key certificate ID 12024, which is ID information for the public key certificate; a certificate validity term 12025; a service provider ID 12026; and a certificate issued time 12027.

[2035] The acceptance number 12017 is arbitrarily generated, by the mobile user terminal of user B, as a number that uniquely represents the telephone card transfer processing. With this number, the mobile user terminal of user A is notified as to whether user B has accepted the card transfer offer 7601. When user B does not accept the card transfer offer 7601, a value of

0 is set as the acceptance number 12017. When user B accepts the card transfer offer 7601, a value other than 0 is set.

[2036] Upon receiving the card transfer offer response 7604, the mobile user terminal of user A displays, on the LCD, the contents of the card transfer offer response 7604 (display the transfer offer response; 7605). When the card transfer offer 7601 is accepted (acceptance number 12017 \neq 0), the mobile user terminal of user A examines the digital signature of the service provider of the user public key certificate 12021 and the validity term. The mobile user terminal generates a card transfer certificate 7606, which is a message that corresponds to a transfer certificate for an electronic telephone card to user B, and transmits it to the mobile user terminal of user B.

[2037] As is shown in Fig. 121A, the digital signature of the electronic payment and the digital signature of user A are provided for the data that consist of a card transfer certificate header 12100, which is header information indicating that the message is the card transfer certificate 7506 and describing the data structure; a presentation card 12101 for an electronic telephone card to be transferred; a card status 12102; a total remaining value 12103; a transfer offer number 12104; an acceptance number 12105; a public key certificate ID 12106 for the user public key certificate of user B; a public key certificate ID 12107 for the user public key certificate of user A; a card ID 12108; and an issued time 12109, which indicates the date on which the card transfer certificate 7606 was issued. These data are closed and addressed to user B, thereby providing the card transfer certificate 7606.

[2038] Upon receiving the card transfer certificate 7606, the mobile user terminal of user B decrypts it and examines the digital signature of user A and the one accompanying the electronic telephone card. Further, the mobile user terminal compares the card ID presented by the card transfer offer 7601 with the card ID 12108, and compares the public key certificate IDs 12106 and 12107 with the public key certificates of users B and A to verify the contents of the card transfer certificate 7606. The mobile user terminal then generates a card transfer receipt 7607, which is a message indicating the electronic telephone card has been received, and transmits the receipt 7607 to the mobile user terminal of user A.

[2039] As is shown in Fig. 121B, the digital signature of user B is provided for the data that consist of a card transfer receipt header 12115, which is header information indicating that the message is the card transfer receipt 7607 and describing the data structure; a card ID 12116; a transfer offer number 12117; an acceptance number 12118; a public key certificate ID 12119 for the user public key certificate of user A; a public key certificate ID 12120 for the user public key certificate of user B; and an issued time 12121, which indicates the date on which the card transfer receipt 7607 was issued.

These data are closed and addressed to user A, thereby providing the card transfer receipt 7607.

[2040] Upon receiving the card transfer receipt 7607, the mobile user terminal of user A decrypts it, and examines the digital signature of user B. Further, the mobile user terminal compares the public key certificate IDs 12119 and 12120 with the public key certificates of users B and A to verify the contents of the card transfer receipt 7607. The mobile user terminal then erases the transferred electronic telephone card from the card list 1714, and registers the card transfer receipt 12122 in use history 1715. At this time, addresses in the object data area at which the transfer offer number, the code information indicating the card transfer process, the issued time for the card transfer receipt 7607 and the card transfer receipt 12122 are stored are assigned to the request number 1840 in the use list 1715, the service code 1841, the use time 1842 and the use information address 1843.

[2041] The mobile user terminal of user A displays, on the LCD, a message indicating the completion of the transfer process (display the transfer process; 7608). The process at the mobile user terminal of user A (sender) is thereafter terminated.

[2042] After transmitting the card transfer receipt 7607, the mobile user terminal of user B displays the received card transfer certificate 12111 on the LCD. In addition, the mobile user terminal displays a dialogue message inquiring whether the transfer process with the service providing server (process for downloading the received electronic telephone card from the service providing system) should be immediately performed (display the transfer certificate; 7609).

[2043] The dialogue message has two operating menus: "transfer process request" and "cancel." When "cancel" is selected, the transfer process performed with the service providing server is canceled, and in the process (data updating process) during which the service providing system updates the data in the mobile user terminal, an electronic telephone card that has been transferred is assigned to the mobile user terminal.

[2044] When user B selects "transfer process request" (transfer process request operation; 7610), based on the card transfer certificate 12111 the mobile user terminal generates a card transfer request 7611, which is a message requesting that the transfer process be performed with the service providing system, and transmits it to the service providing system via digital wireless telephone communication.

[2045] As is shown in Fig. 122A, the digital signature of user B is provided for the data that consists of a card transfer request header 12200, which is header information indicating that the message is the card transfer request 7611 and describing the data structure; a decrypted card transfer certificate 12201 (12111); the user ID 12202 of user B; and an issued time 12203, which indicates the date when the card transfer request

7611 was issued. These data are closed and addressed to the service provider, thereby providing the card transfer request 7611.

[2046] Upon receiving the card transfer request 7611, the user processor of user B of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor generates a service director processor to form a process group for processing the card transfer request 12204.

[2047] The service director processor, first refers to the user list 5200 and specifies the recipient (user B) and the sender (user A) of the transfer process by employing the public key certificate IDs 12106 and 12107 in the card transfer certificate 12201 that is included in the card transfer request 12204. The service director processor examines the digital signature of the user A and the digital signature accompanying the electronic telephone card, which are provided for the card transfer certificate 12201, and verifies the validity of the card transfer certificate 12201. Following this, the service director processor erases the electronic telephone card to be transferred from the card list 4612 of the user A that is stored in the user information server 902. Then, the service director processor changes the card signature private key and card signature public key pair and the card certificate for a new key pair and a card certificate, and also changes the card status and the total remaining value to the card status 12102 and to the total remaining value 12103 for the card transfer certificate 12201. The service director processor generates an electronic telephone card received from user A, and enters it in the card list 4612 for the user B.

[2048] When the electronic telephone card that is to be transferred has already been registered, the service director processor updates the registered card list 5502 holding the electronic telephone card. Specifically, the user ID 5518, the user public key 5519, the registered card certificate address 5520, the telephone micro-check list address 5521 and the former user information address 5522, all of which are in the registered card list 5502, are updated (to the information for user B). The old information (information for user A) is pointed to at the former user information address 5522 as former user information 5523..

[2049] The service director processor generates a telephone card transfer message 12226, which includes an electronic telephone card transferred from user A. The user processor of user B closes the message 12226 and addresses it to the user B, and transmits it as a telephone card transfer message 7612 to the mobile user terminal of user B via digital wireless telephone communication.

[2050] As is shown in Fig. 122C, the digital signature of the service provider is provided for the data that consist of a telephone card transfer header 12219, which is header information indicating that the message is the card transfer 7612 and describing the data structure; a

transfer number 12220, which is an arbitrarily generated number that represents the transfer process in the service providing system; transfer information 12221; an acceptance number 12222; an electronic telephone card 12223, which is transferred; a service provider ID 12224; and an issued time 12225, which indicates the date when the telephone card transfer message 7612 was issued. These data are closed and addressed to the user B, thereby providing the card transfer message 7612.

[2051] The transfer information 12221 is information concerning the electronic telephone card transfer process performed by the service providing system, and is accompanied by the digital signature of the service provider. The mobile user terminal of user B decrypts the received telephone card transfer message 7612 and examines the digital signature, registers the electronic telephone card 12223 in the card list 1714, and displays the electronic telephone card on the LCD (display the electronic telephone card; 7613). The card transfer process is thereafter terminated.

[2052] An explanation will now be given for the contents of messages that are exchanged by the devices during the electronic telephone card installation processing.

[2053] In Fig. 79 are shown procedures for the exchange of messages by the devices during the electronic telephone card installation processing, and in Figs. 127A and 127B, and 128A and 128B are shown the contents of messages that are exchanged during the electronic payment installation processing.

[2054] First, when the user performs an electronic telephone card installation operation 7900, the mobile user terminal generates an electronic telephone card installation request 7901, and transmits it to the service providing system 110 via digital wireless telephone communication.

[2055] As is shown in Fig. 127A, the digital signature of the user is provided for the data that consists of an electronic telephone card installation request header 12700, which is header information indicating that the message is the electronic telephone card installation request 7901 and describes the data structure; an installation card number 12701 and an installation number 12702, which are entered by a user; a request number 12703, which is an arbitrarily generated number that uniquely represents the electronic telephone card installation process; a user ID 12704; and an issued time 12705, which indicates the date when the electronic telephone card installation request 7901 was issued. These data are closed and addressed to the service provider, thereby providing the electronic telephone card installation request 7901.

[2056] Upon receiving the electronic telephone card installation request 7901, the user processor of the service providing system 110 decrypts it and examines the digital signature, and transmits it to the service manager processor. The service manager processor gener-

ates a service director processor to form a process group for processing the electronic telephone card installation request 12706.

[2057] First, the service director processor refers to the installation card list that is indicated by the installation card list address 5243 for the telephone card issuer list 5205, and specifies a telephone card issuer who issues a telephone card that is represented by the installation number 12701. The service director processor generates a telephone card installation request 12717, which is a message requesting that the telephone card issuer issue a telephone card using the installation card. The telephone card issuer processor closes the request 12717 and addresses it to the telephone card issuer, and transmits it as a telephone card installation request 7902 to the telephone card issuing system 108.

[2058] As is shown in Fig. 127B, the digital signature of the service provider is provided for the data that consist of a telephone card installation request header 12710, which is header information indicating that the message is the telephone card installation request 7902 and describing the data structure; an installation card number 12711; an installation number 12712; a request number 12713; a customer number 12714, which uniquely represents a user for the telephone card issuer; a service provider ID 12715; and an issued time 12716, which indicates the date when the telephone card installation request 7902 was issued. These data are closed and addressed to the telephone card issuer, thereby providing the telephone card installation request 7902.

[2059] Upon receiving the telephone card installation request 7902, the telephone card issuing system 109 decrypts it and examines the digital signature. The telephone card issuing server 1300 compares the installation card number 12711 and the installation number 12712, which are included in the telephone card installation request 7902, with the management information for the issued electronic telephone card installation card that is stored in the telephone card issuing information server 1302. The telephone card issuing server 1300 then updates the data in the customer information server 1302 and the telephone card issuing information server 1303. Furthermore, the telephone card issuing server generates telephone card data (12806) for a requested telephone card, and transmits, to the service providing system, an electronic telephone card installation commission 7903, which is a message requesting the installation of an electronic telephone card that corresponds to the requested telephone card.

[2060] As is shown in Fig. 128A, the digital signature of the telephone card issuer is provided for the data that consists of an electronic telephone card installation commission header 12800, which is header information indicating that the message is the electronic telephone card installation commission 7903 and describing the data structure; a transaction number 12801, which is an

arbitrarily generated number that uniquely represents the transaction with a user; telephone card issuing information 12802; a request number 12803; card code 12804, which indicates the type of electronic telephone card that is to be issued; a template code 12805, which indicates a template program for an electronic telephone card to be issued; telephone card data 12806; representative component information 12807; a telephone card issuer ID 12808; and an issued time 12809, which indicates the date when the electronic telephone card installation commission 7903 was issued. These data are closed and addressed to the service provider, thereby providing the electronic telephone card installation commission 7903.

[2061] The telephone card issuing information 12802 is information concerning the telephone card issuing process performed by the telephone card issuing system, and is accompanied by the digital signature of the telephone card issuer.

[2062] The telephone card data 12806 is telephone card information issued by the telephone card issuer, wherein the digital signature of the telephone card issuer accompanies the data that consists of the card ID 12814, the telephone card information 12815 and the card ID 12816.

[2063] The telephone card issuer processor of the service providing system decrypts the received electronic telephone card installation commission 7903 and examines the digital signature, and transmits the commission 7903 to the service director processor. In accordance with the electronic telephone card installation commission 12810, the service director processor generates an electronic telephone card to be issued to a user, using the same procedures as are used for the telephone card purchase processing, and also generates an electronic telephone card installation message 12815, which is a message directing that the electronic telephone card be installed in the mobile user terminal. The user processor closes the electronic telephone card installation message 12855 and addressees it to a user, and transmits it as an electronic telephone card installation message 7904 to the mobile user terminal via digital wireless telephone communication.

[2064] As is shown in Fig. 128B, the digital signature of the service provider is provided for the data that consists of an electronic telephone card installation header 12817, which is header information indicating that the message is the electronic telephone card installation message 7904 and describing the data structure; a transaction number 12818; telephone card issuing information 12819, which concerns the telephone card issuing process performed by the telephone card issuing system; telephone card issuing information 12820, which concerns the telephone card issuing process performed by the service providing system; a request number 12821; generated electronic telephone card data 12822; a service provider ID 12823; and an issued time 12824, which indicates the date when the elec-

tronic telephone card installation message 7904 was issued. These data are closed and addressed to the user, thereby providing the electronic telephone card installation message 7904. The telephone card issuing information 12819 and the telephone card issuing information 12820 are accompanied by the digital signatures of the telephone card issuer and the service provider.

[2065] The mobile user terminal decrypts the received electronic telephone card installation message 7904 and examines the digital signature, registers, in the card list 1714, the electronic telephone card included in the electronic telephone card installation request 7904, and displays the installed electronic telephone card on the LCD (display the electronic telephone card; 7905).

[2066] An explanation will now be given for the contents of messages that are exchanged by the devices during the real credit clearing process for electronic credit card service.

[2067] In Fig. 84 are shown procedures for the exchange of messages by the devices during the real credit clearing processing, and in Figs. 135A to 135F, 136A to 136C, and 137A and 137B are shown the contents of the messages that are exchanged by the devices during the real credit clearing processing.

[2068] First, when the merchant presses the switch on the cash register for the credit card clearing (8401), the merchant terminal 102 or 103 generates multiple types of payment offer responses 8406 and enters the wait state for a payment offer 8405.

[2069] The payment offer responses 8406 are those used when an amount of payment entered by a user is insufficient, when a credit card or a payment option designated by the user is not available, or when the payment offer 8405 is accepted.

[2070] When the user performs a payment operation 8404, the mobile user terminal 100 generates the payment offer 8405 and transmits it to the merchant terminal 102 or 103 via infrared communication.

[2071] As is shown in Fig. 135A, the digital signature of a user is provided for data that consists of a payment offer header 13500, which is header information indicating that the message is the payment offer 8405 and describing the data structure; a payment service code 13501, which is a service code used to identify the type of electronic credit card designated by a user; a request number 13502, which is an arbitrarily generated number that uniquely represents the transaction with a merchant; an amount of payment 13504, which is entered by a user; a payment option code 13505, which is a payment option, such as the number of payments, entered by a user; an effective period 13506 for the payment offer 8405; and an issued time 13507, which indicates the date on which the payment offer 8405 was issued. Thus, the payment offer 8405 is provided.

[2072] Upon receiving the payment offer 8405, the merchant terminal 102 or 103 examines the payment service code 13501, the amount of payment 13504 and the payment option 13505, and selects an appropriate

payment offer response 8406 from among multiple types of responses 8406 and transmits it to the mobile user terminal via infrared communication. Further, the terminal 102 or 103 generates an authorization request 8409 and transmits it to the merchant processor of the service providing system 110.

[2073] As is shown in Fig. 135B, the digital signature of a merchant is provided for the data that consists of a payment offer response header 13508, which is header information indicating that the message is the payment offer response 8406 and describing the data structure; a response message 13509, which is displayed on the LCD 303 when the mobile user terminal 100 receives the payment offer response 8406; a transaction number 13510, which is an arbitrarily generated number that uniquely represents the transaction with a user; an amount of sales 13511; a service provider telephone number 13512, which is the telephone number of the service providing system in the service area of the merchant; an effective period 13513 for the payment offer response 8406; a merchant ID 13514; and an issued time 13515, which indicates the date on which the payment offer response 8406 was issued. In this fashion, the payment offer response 8406 is provided.

[2074] The service provider telephone number 13512 is accompanied by the digital signature of the service provider. The response message 13509 is a text message that is optionally selected by the merchant, and may not always be selected.

[2075] When the amount of payment designated by the user is insufficient, or when a credit card or a payment option entered by the user can not be accepted, the merchant terminal sets for the transaction number 13510 a value of "0," thus notifying the mobile user terminal that the payment offer 8405 can not be accepted.

[2076] As is shown in Fig. 135C, the digital signature of a merchant is provided for the data that consists of an authorization request header 13516, which is header information indicating that the message is the authorization request 8409 and describing the data structure; a payment offer 8405; a payment offer response 8406; an accounting machine ID 13517; a merchant ID 13518; and an issued time 13519, which indicates the date on which the authorization request 8409 was issued. These data are closed and addressed to the service provider, thereby providing the authorization request 8409.

[2077] The mobile user terminal 100 receives the payment offer response 8406, compares the amount of payment 13504 with the amount of sale 13511, generates a payment request 8410, and transmits it to the user processor of the service providing system via digital wireless telephone communication.

[2078] As is shown in Fig. 135D, the digital signature of a user is provided for the data that consists of a payment request header 13524, which is header information indicating that the message is the payment request 8410 and describing the data structure; a payment offer

8405; a payment offer response 8406; a user ID 13525; and an issued time 13526, which indicates the date on which the payment request 8410 was issued. These data are closed and addressed to the service provider, thereby providing the payment request 8410.

[2079] Either the transmission of the authorization request 8409 by the merchant terminal 102 or 103, or the transmission of the payment request 8410 by the mobile user terminal may be performed first, or the two of them may be performed at the same time.

[2080] The merchant processor and the user processor of the service providing system 110 receive the authorization request 8409 and the payment request 8410, decrypt them and examine the digital signatures, and transmit an authorization request 13520 and a payment request 13527 to the service manager processor. The service manager processor compares the request number, the transaction number and the merchant ID to obtain a correlation between the authorization request and the payment request, and generates the service director processor to form a process group for handling the authorization request 13520 and the payment request 13527. The service director processor compares the contents of the authorization request 13520 with those of the payment request 13527, authorizes the user and generates an authorization response 13540. The merchant processor closes the response 13540, addresses it to the merchant and transmits it as an authorization response 8411 to the merchant terminal.

[2081] As is shown in Fig. 135E, the digital signature of a service provider is provided for the data that consists of an authorization response header 13531, which is header information indicating that the message is the authorization response 8411 and describing the data structure; a transaction number 13532; an authorization number 13533, which is an arbitrarily generated number that uniquely represents the authorization processing; user personal data 13535; a customer number 13536; an effective period 13537, which designates a period during which the authorization response 8411 is effective; a service provider ID 13538; and an issued time 13539, which indicates the date on which the authorization response 8404 was issued. These data are closed and addressed to the merchant, thereby providing the authorization response 8411.

[2082] When, as the result of the authorization process, it is determined that the credit condition of the user is not satisfactory, the user personal data 13534 are not set. The customer number 13536 is set only when a transaction was previously made between the user and the merchant through an electronic commerce service.

[2083] The merchant terminal 102 or 103 decrypts the received authorization response 8411 and examines the digital signature, and displays the results of the authorization process on the LCD.

[2084] When an operator (merchant) performs a clearing request operation 8413, the merchant terminal gen-

erates a clearing request 8415 and transmits it to the merchant processor. As is shown in Fig. 135F, the digital signature of a merchant is provided for the data that consist of a clearing request header 13544, which is header information indicating that the message is the clearing request 8415 and describing the data structure; a payment offer 8405; a payment offer response 8406; an authorization number 13545, which is issued by the service providing system 110; an effective period 13546, which indicates a period during which the clearing request 8415 is effective; an accounting machine ID 13547; a merchant ID 13548; and an issued time 13549, which indicates the date on which the clearing request 8415 was issued. These data are closed and addressed to the service provider, thereby providing the clearing request 8415.

[2085] Upon receiving the clearing request 8415, the merchant processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing request 8450 to the service director processor. The service director processor compares the clearing request 8450 with the payment request 8427, and generates a clearing request 13610 for the transaction processor. The transaction processor closes the request 13610, addresses it to the transaction processor, and transmits it as a clearing request 8416 to the transaction processing system.

[2086] As is shown in Fig. 136A, the digital signature of a service provider is provided for data that consist of a clearing request header 13600, which is header information indicating that the message is the clearing request 8416 and describing the data structure; a user clearing account 13601, which indicates a credit card that corresponds to the payment service code designated by the user; a request number 13602, which is issued by the mobile user terminal 100; an amount of payment 13603; a payment option code 13604; a merchant clearing account 13605, which indicates a clearing account for the merchant; a transaction number 13606, which is issued by the merchant terminal; an effective period 13607, which indicates the period wherein the clearing request 8416 is effective; a service provider ID 13608; and an issued time 13609, which indicates the date on which the clearing request 8416 was issued. These data are closed and addressed to the transaction processor, thereby providing the clearing request 8416.

[2087] The transaction processing system 106 receives the clearing request 8416, decrypts it and examines the digital signature, and performs the clearing process. Then, the transaction processing system 106 generates a clearing completion notification 8417 and transmits it to the service providing system 110.

[2088] As is shown in Fig. 136B, the digital signature of a transaction processor is provided for data that consist of a clearing completion notification header 13614, which is header information indicating that the message is the clearing completion notification 8417 and describ-

ing the data structure; a clearing number 13615, which is an arbitrarily generated number that uniquely represents the clearing process performed by the transaction processing system 106; a user clearing account 13616; a request number 13617; an amount of payment 13618; a payment option code 13619; a merchant clearing account 13620; a transaction number 13621; clearing information 13622 for a service provider that is accompanied by the digital signature of the transaction processor; clearing information 13623 for a merchant that is accompanied by the digital signature of the transaction processor; clearing information 13624 for a user that is accompanied by the digital signature of the transaction processor; a transaction processor provider ID 13625; and an issued time 13626, which indicates the date on which the clearing completion notification was issued. These data are closed and addressed to the service provider, thereby providing the clearing completion notification 8417.

[2089] Upon receiving the clearing completion notification 8417, the transaction processor processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a clearing completion notification 13627 to the service director processor. Upon receiving the clearing completion notification 13627, the service director processor generates a clearing completion notification 13637 for the merchant. The merchant processor closes the clearing completion notification 13637, addresses it to the merchant, and transmits it to the merchant terminal as a clearing completion notification 8418 for the merchant.

[2090] As is shown in Fig. 136C, the digital signature of a service provider is provided for data that consist of a clearing completion notification header 13631, which is header information indicating that the message is the clearing completion notification 8418 and describing the data structure; a clearing number 13632; clearing information 13623 for a merchant that is accompanied by the digital signature of the transaction processor; a customer number 13633, which is an arbitrarily generated number that uniquely represents a user for a merchant; a decrypted clearing request 13550; provided service information 13634, which concerns the process performed by the service providing system 110; a service provider ID 13635; and an issued time 13636, which indicates the date on which the clearing completion notification 8418 was issued. These data are closed and addressed to the merchant, thereby providing the clearing completion notification 8418. The provided service information 13634 is set optionally by the service provider, and may not always be set.

[2091] Upon receiving the clearing completion notification 8418, the merchant terminal decrypts it and examines the digital signature, and generates a receipt 8419 and transmits it to the merchant processor.

[2092] As is shown in Fig. 137A, the digital signature of a merchant is provided for data that consist of a receipt header 13700, which is header information indi-

cating that the message is the receipt 8419 and describing the data structure; an item name 13701, which indicates a product that is sold; sales information 13702, which is additional information concerning the transaction transmitted by the merchant to the user; a clearing number 13703; transaction information 13704; a payment offer 8405; an accounting machine ID 13705; a merchant ID 13706; and an issued time 13707, which indicates the date on which the receipt 8419 was issued. These data are closed and addressed to the service provider, thereby providing the receipt 8419. The sales information 13702 is set optionally by the merchant, and may not always be set.

[2093] Upon receiving the receipt 8419, the merchant processor of the service providing system 110 decrypts it and examines the digital signature, and transmits a receipt 13708 to the service director processor. The service director processor employs the receipt 13708 to generate a receipt 13717 for a user. The service director processor closes the receipt 13717 and addresses it to the user, and transmits it as a receipt 8421 to the mobile user terminal 100 via digital wireless telephone communication.

[2094] As is shown in Fig. 137B, the digital signature of a service provider is provided for data that consist of a receipt header 13712, which is header information indicating that the message is the receipt 8421 and describing the data structure; a user ID 13713; a decrypted receipt 13708; clearing information 13709 for a user that is accompanied by the digital signature of the transaction processor; provided service information 13714, which concerns the process performed by the service providing system 110; a service provider ID 13715; and an issued time 13716, which indicates the date on which the receipt 8421 was issued. These data are closed and addressed to the user, thereby providing the receipt 8421. The provided service information 13713 is set optionally by the service provider, and may not always be set.

[2095] Upon receiving the receipt 8421, the mobile user terminal 100 decrypts it and examines the digital signature, and displays the contents on the LCD 303. The real credit clearing process is thereafter terminated.

[2096] In the mobile user terminal 100, the ROM 1501 and the EEPROM 1503 may be replaced by ferroelectric nonvolatile memory as a memory device for storing a program executed by the CPU 1500 and the public key of the service provider. This memory device can store data without a battery being required, while like EEPROM or flash memory, data can be written to it. In addition, the reading and writing speeds of the ferroelectric nonvolatile memory are higher than those of EEPROM and flash memory, and the power consumption is low.

[2097] When the ferroelectric nonvolatile memory is employed instead of the ROM 1501 and the EEPROM 1503, in the same manner, for example, as in the data updating process, the program for the mobile user ter-

minal 100 can be extensively updated, and the public key of the service provider can be periodically updated within a comparatively short period of time with little battery service life loss.

[2098] Furthermore, a ferroelectric nonvolatile memory may be used as the RAM 1502 to store the data that are to be processed and the data that are processed by the CPU 1500. Since data are not lost even when the battery power has been exhausted, a data backup process is not required, and the power supply required for storing the data resident in the RAM is not needed. As a result, the power consumed by the mobile user terminal can be reduced.

[2099] Also, a ferroelectric nonvolatile memory may be used instead of the ROM 3001 and the EEPROM 3003 in the merchant terminal 103, or the RAM 3002. In this case, the same effects are acquired as are obtained with the mobile user terminal 100.

[2100] In the above explanation, the mobile user terminal 100, the gate terminal 101 and the merchant terminals 102 and 103, which together constitute the mobile electronic commerce system, include an optimal hardware arrangement with which to implement the individual functions needed to provide the mobile electronic commerce service. These components can be constituted by a wireless telephone communication function, an infrared communication function, and a computer that comprises a display device, a keyboard (or an input pen), a microphone and a loudspeaker, and that further comprises a bar code reader for the merchant terminal 103.

[2101] In this case, functionally corresponding hardware components of the mobile user terminal 100, the gate terminal 101, or the merchant terminal 102 or 103 are modified for inclusion in a program for the hardware components that are not included in the computer (e.g., a data codec, a cryptographic processor and a logic control unit). This program, together with a program stored in the ROM 1501 (or 2201, 2601 or 3001), is converted so that it can be operated by the OS (Operating System) of a personal computer. The resultant program is then stored at a location (e.g., on a hard disk) where it can be accessed by the computer.

[2102] A second embodiment of the present invention will now be described while referring to Figs. 139 and 140.

[2103] In the mobile electronic commerce system in the second embodiment, instead of the EEPROM 1503 an SIM (Subscriber Identify Module) card is employed for the mobile user terminal 100 in the first embodiment.

[2104] Figs. 139A and 139B are a front view and a rear view of a mobile user terminal 13900 for the second embodiment, and Fig. 140 is a block diagram illustrating the arrangement of the mobile user terminal 13900. The arrangement of the mobile user terminal 13900 is the same as that of the mobile user terminal 100, except that an SIM card 14000 and an SIM card reader/writer 14001 are provided instead of the EEPROM 1503. The

external appearance of the mobile user terminal 13900 is also the same as that of the mobile user terminal 100, except that an SIM card attachment section 13901 is provided on the reverse side for attaching the SIM card 14000.

[2105] The same information as is stored in the EEPROM 1503 in the first embodiment is stored in the non-volatile memory of the SIM card 149000: the terminal ID and the telephone number of the mobile user terminal 13900 when used as a wireless telephone terminal; a user ID; a user code number; a private key and a public key used for a digital signature; a service provider ID; the telephone number of the service providing system 110 (which is accompanied by the digital signature of the service provider); and the public key of the service provider.

[2106] The SIM card 14000 can be carried separately from the mobile user terminal 13900. But without the SIM card 14000, if it has been removed, the mobile user terminal 13900 can not be operated. When the SIM card 14000 is attached to the SIM card reader/writer 14001, the CPU 1500 of the mobile user terminal 13900 accesses the information stored on the SIM card 14000 via the SIM card reader/writer 14001 and a bus 1529. The mobile user terminal 13900 then performs the same operations as does the mobile user terminal 100 in the first embodiment.

[2107] Further, to remove the SIM card 14000 from the mobile user terminal 13900, the following operation must be performed.

[2108] First, when a user depresses the power switch and holds it down for five seconds (removal operation 1 for the SIM card 14000), the mobile user terminal 13900 displays, on the LCD 303, a dialogue message requesting confirmation that the SIM card will be removed. Then, when the user depresses the execution switch (removal operation 2 for the SIM card 14000), the mobile user terminal 13900 performs a data updating process with the service providing system 110, and uploads the data from the RAM 1502 of the mobile user terminal 13900 to the user information server 902. When the user removes the SIM card 14000 from the SIM card reader/writer 14001 (removal operation 3 for the SIM card 14000), the mobile user terminal 13900 deletes all the data held in the RAM 1502.

[2109] Specifically, when the SIM card is removed from the mobile user terminal, the data, such as those for the electronic ticket and electronic payment card, that are stored in the RAM of the mobile user terminal are uploaded to the user information server 902 of the service providing system 110.

[2110] The following operation is performed when the SIM card 14000 is attached to the mobile user terminal 13900.

[2111] When the SIM card 14000 is connected to the SIM card reader/writer 14001, the mobile user terminal 13900 displays, on the LCD 303, a screen which permits the entry of a code number. When the user enters

the code number and presses the execution switch, the code number stored in the nonvolatile memory of the SIM card 14000 is compared with the code number that was entered. When the two numbers do not match, the mobile user terminal 13900 again displays on the LCD 303 which permits the entry of the code number. When the two code numbers match, access to the SIM card 14000 is permitted. The mobile user terminal 13900 reads, from the SIM card 14000, the user ID, the private key used for the digital signature, the telephone number of the service providing system 110 and the public key of the service provider, and performs a data updating process with the service providing system 110 in order to update the data in the RAM 1502 of the mobile user terminal 13900. At this time, the data for the mobile user terminal in the user information server 902 are stored in the RAM 1502 of the mobile user terminal 13900, in accordance with the user ID stored on the SIM card 14000.

[2112] Specifically, the data for the mobile user terminal, such as the data for the electronic ticket or for the electronic payment card that are uploaded to the user information server 902 of the service providing system 110, are downloaded to the mobile user terminal to which the SIM card is attached. When, for example, an SIM card is attached to a mobile user terminal that differs from the mobile user terminal to which the SIM card was previously attached, the same data as those stored in the RAM of the mobile user terminal to which the SIM card was previously attached are stored in the RAM of the mobile user terminal to which the SIM card is currently attached.

[2113] Therefore, the user can carry the SIM card 14000 on which the user ID is stored, and can employ an arbitrary mobile user terminal as his or her own by attaching the SIM card to that mobile user terminal.

[2114] In the mobile user terminal 13900, not only the areas used for storing the user ID and the code number, but also areas that correspond to the basic program area 1700 of the RAM 1502, the service data area 1701, the user area 1702 and the temporary area 1704 may be provided for the nonvolatile memory of the SIM card 14000, so that the data stored in these areas in the RAM 1502 may be stored in the nonvolatile memory of the SIM card 14000. In this case, the data for the electronic ticket or the electronic payment card are stored in the nonvolatile memory of the SIM card 14000, and the RAM 1502 is a work area that is used by the CPU 1500 when executing a program.

[2115] Since the data stored in the RAM 1502, other than in the work area 1703 of the mobile user terminal 100 of the first embodiment, are held in the nonvolatile memory of the SIM card 14000, the data updating process, which is performed when the SIM card is attached and removed, is not required, and as a power source for holding data is also not required, the power consumed by the mobile user terminal can be reduced.

[2116] A ferroelectric memory may be used as the

nonvolatile memory for the SIM card 14000. Since the reading and writing speeds of the ferroelectric nonvolatile memory are higher than are those of EEPROM and flash memory, and since the power consumption is low, the processing speed of the mobile user terminal can be increased and its power consumption can be reduced.

[2117] A third embodiment will now be described while referring to Figs. 141 to 143.

[2118] According to the third embodiment, a mobile electronic commerce system is provided that includes an IC card reader/writer and that employs, as a mobile user terminal, a portable wireless telephone terminal wherein an electronic ticket, an electronic payment card or an electronic telephone card that the user obtains is stored in an IC card loaded into the telephone terminal.

[2119] Figs. 141A and 141B are a front view and a rear view of a mobile user terminal 14100 according to the third embodiment, and Fig. 142 is a block diagram illustrating the arrangement of the mobile user terminal 14100. The external appearance of the mobile user terminal 13900 is the same as that of the mobile user terminal 100, except that an IC card insertion slot 14101 is formed in the reverse side for loading the IC card 14100. The arrangement of the mobile user terminal 14100 is the same as that of the mobile user terminal 100, except that the cryptographic processor 1505 is replaced by an IC card reader/writer 14200. When the IC card 14102 is loaded into the IC card reader/writer 14200, the mobile user terminal 14100 performs the same operations as does the mobile user terminal 100 in the first embodiment for the other devices, such as the service providing system 110, the gate terminal 101, the merchant terminals 102 and 103, the automatic vending machine 104 and the switching center 105.

[2120] It should be noted that the mobile user terminal 14100 performs the following operation when the IC card 14102 is loaded therein.

[2121] When the IC card 14102 is loaded in the IC card reader/writer 14200, the mobile user terminal 14100 displays, on the LCD 303, a screen permitting the entry of a code number. When the user enters the code number and presses the execution switch, the code number stored in the IC card 14102 is compared with the code number that was entered. When the two numbers do not match, the mobile user terminal 14100 again displays, on the LCD 303, the screen permitting the entry of a code number. When the two code numbers match, access to the IC card 14102 is permitted.

[2122] For the mobile user terminal 14100, the user ID and the user code number, the private key and the public key used for a digital signature, the service provider ID, the telephone number of the service providing system 110 and the public key of the service provider are stored in the IC card 14102, while the terminal ID and the telephone number of the mobile user terminal 14100 when used as a wireless telephone terminal are stored in the EEPROM 1503.

[2123] In addition, an additional program and the data

for the electronic ticket or the electronic payment card, which are stored in the basic program area 1700, the service data area 1701, the user area 1702 and the temporary area 1704 in the RAM 1502 of the mobile user terminal 100 of the first embodiment, are stored on the IC card 14102 of the mobile user terminal 14100. The RAM 1502 of the mobile user terminal 14100 serves as a work area that is used by the CPU 1500 when executing a program.

[2124] Furthermore, the mobile user terminal 14100 employs the IC card 14100 loaded into the IC card reader/writer 14200 to perform one part of the data processing for the messages that are exchanged with the service providing system 110, the gate terminal 101, the merchant terminals 102 and 103, the automatic vending machine 104 or the switching center 105 for the mobile electronic commerce service.

[2125] Fig. 143 is a block diagram illustrating the arrangement of the IC card 14102.

[2126] The IC card 14102 includes two interfaces, one for a contact type IC card and one for a non-contact IC card. This IC card comprises: a CPU (Central Processing Unit) 14300, which processes data to be transmitted and data that are received in accordance with a program stored in a ROM (Read Only Memory) 14301, and which controls the other components across a bus 14318; a RAM (Random Access Memory) 14302, in which are stored data that are to be processed and that are being processed by the CPU 14300; an FeRAM (Ferroelectric Random Access Memory) 14303, in which are stored a user ID and a code number for a user, a private key and a public key for a digital signature, a service provider ID, the telephone number of the service providing system 110, the public key of the service provider, and an additional program or data such as those for an electronic ticket or for an electronic payment card, which are stored in the basic program area 1700, the service data area 1701, the user area 1702 and the temporary area 1704 of the RAM 1502 for the first embodiment; a cryptographic processor 14304, which encrypts or decrypts data under the control of the CPU 14300; an input/output circuit 14305, which converts and controls a signal that is input or output at a contact 14306 of a non-contact IC card under the control of the CPU 14300; and an RF modem 14307, which converts and controls radio waves that are input or output by an antenna 14308 of a non-contact IC card under the control of the CPU 14300.

[2127] The cryptographic processor 14304, which corresponds to the cryptographic processor 1505 of the mobile user terminal 100 in the first embodiment, includes an encryption and decryption function that uses a secret key method and an encryption and decryption function for a public key system. The cryptographic processor 14304 employs the cryptograph method and keys that are set by the CPU 14300 to encrypt or decrypt data as designated by the CPU 14300. The cryptographic function of the cryptographic

processor 14304 is employed for the process for providing a digital signature for a message or the process for closing the message, and the process for decrypting the closed message or the process for verifying a digital signature accompanying the message.

[2128] To transmit, via a digital wireless telephone communication, a message that is closed and is accompanied by a digital signature, first, the CPU 14300 employs the cryptographic processor 14304 to perform the digital signature provision process and the message closing process, and transmits the resultant message to the input/output circuit 14305. The message, which is closed and is accompanied by the digital signature, is converted into an electric signal by the input/output circuit 14305, and the electric signal is output at the contact point 14306. Through the IC card reader/writer 14200 and the bus 1529, the CPU 1500 reads, as a message, the electric signal that is output at the contact 14306. The CPU 14300 employs the data codec 1506 to encode the message that is closed and accompanied by the digital signature to obtain a data form for digital wireless telephone communication, and transmits the coded message via the control logic unit 1508 to the channel codec 1513.

[2129] When a message that is closed and is accompanied by a digital signature is received via digital wireless telephone communication, the CPU 1500 reads the received message from the channel codec 1513 through the control logic unit 1508, employs the data codec 1506 to decrypt the received message, and transmits the decrypted message to the IC card 14102 via the bus 1529 and the IC card reader/writer 14200. The CPU 14300 receives a message via the contact point 14306 and the input/output circuit 14305, and employs the cryptographic processor 14304 to decrypt the closed and encrypted message and to examine the digital signature accompanying the message.

[2130] Similarly, to transmit via infrared communication a message that is closed and is accompanied by a digital signature, first, the CPU 14300 employs the cryptographic processor 14304 to perform the digital signature provision process and the message closing process, and transmits the resultant message to the input/output circuit 14305. The message that is closed and is accompanied by the digital signature is converted into an electric signal by the input/output circuit 14305, and the electric signal is output at the contact point 14306. Through the IC card reader/writer 14200 and the bus 1529, the CPU 1500 reads, as a message, the electric signal that is output at the contact 14306. The CPU 14300 employs the data codec 1506 to encode the message that is closed and is accompanied by the digital signature to obtain a data form for infrared communication, and transmits the coded message to the infrared communication module 1507.

[2131] When a message that is closed and is accompanied by a digital signature is received via infrared communication, the CPU 1500 reads the received mes-

sage from the infrared communication module 1507, employs the data codec 1506 to decrypt the received message, and transmits the decrypted message to the IC card 14102 via the bus 1529 and the IC card reader/writer 14200. The CPU 14300 receives a message via the contact point 14306 and the input/output circuit 14305, and employs the cryptographic processor 14304 to decrypt the closed and encrypted message and to examine the digital signature accompanying the message.

[2132] In Fig. 144 is shown a memory map for the FeRAM 14303. The FeRAM 14303 includes five areas: a security area 14400, a basic program area 14401, a service data area 14402, a user area 14403 and a temporary area 14404. The security area 14400 is used to store a user ID, a user code number, a private key and a public key for a digital signature, a service provider ID, the telephone number of the service providing system (that is accompanied by the digital signature of the service provider), and the public key of the service provider. The basic program area 14401, the service data area 14402, the user area 14403 and the temporary area 14404 correspond to the basic program area 1700, the service data area 1701, the user area 1702 and the temporary area 1704 in the RAM 1502 of the mobile user terminal 100 for the first embodiment, and the same data are stored in these areas as are stored in the first embodiment. That is, all the information used for the mobile electronic commerce service, such as the user ID, the keys for the digital signature, or the electronic ticket or the electronic payment card that the user obtained, are stored on the IC card 14102.

[2133] Therefore, the user can carry the IC card 14102 in which the user ID is stored, and can perform the electronic commerce service function, while using an arbitrary mobile user terminal that is regarded as his or her own, by loading the IC card 14102 into that mobile user terminal.

[2134] In addition, since the mobile user terminal 14100 can not access the IC card 14102 when it is not loaded, the mobile user terminal 14100 can not process message data obtained through the mobile electronic commerce service. Therefore, in this case, the mobile electronic commerce service function of the mobile user terminal 100 can not be employed, and only the digital wireless telephone function can be used.

[2135] In Fig. 141C is shown the screen that is displayed on the LCD 303 in the digital wireless telephone mode when the IC card 14102 is not loaded, and in Fig. 141D is shown the screen that is displayed on the LCD 303 in the credit card mode when the IC card 14102 is loaded.

INDUSTRIAL USABILITY

[2136] As is apparent from the above description, the mobile electronic commerce system according to the present invention can download to the electronic wallet

an electronic negotiable card, such as a payment card, a telephone card or a ticket, through the communication means, and can easily obtain such a card. When the electronic payment card, the electronic telephone card or the electronic ticket is to be used, the settlement process or the examination process is quickly and precisely performed, so that safety and usability for a business transaction can be provided.

[2137] The performance of an illegal activity during a business transaction can be prevented, and the secrecy of personal information can be maintained.

[2138] The electronic payment card, the electronic telephone card and the electronic ticket can be delivered along a distribution route as a form of printed matter or as a recording medium, and wide distribution is possible.

[2139] In addition, the usability in the mobile environment can be improved, and, particularly in the invention cited in claims 24 and 25, a system appropriate to the environment in which it is to be used can be obtained.

[2140] According to the invention cited in claim 27, cash is not required to purchase a product from an automatic vending machine, and the usability can be improved.

[2141] According to the invention cited in claim 28, the operator is able to manipulate the electronic payment card clearing means and to present, to a person in charge, the data stored in the electronic payment card clearing means. Thus, the usability of the electronic payment card clearing means is improved.

[2142] According to the invention cited in claim 30, since the calculation of the price of a product and the settlement process can be preformed, the usability is improved.

[2143] According to the invention cited in claim 31, since the process beginning with the promotion of a product and continuing until the product is sold is automated, the usability is improved.

[2144] According to the invention cited in claim 32, the provision of a communication service and the collection of a communication charge for that service can be performed at the same time, and the collection rate for the communication charge can be improved.

[2145] According to the invention cited in claim 33, the operator is able to operate the electronic ticket means and to present, to a person in charge, the data stored in the electronic ticket means. Thus, the usability of the electronic ticket means is improved.

[2146] According to the invention cited in claim 34, the service providing means can efficiently manage the electronic wallet and the electronic payment card clearing means, and can provide the electronic payment card service, the electronic telephone card service and the electronic ticket service.

[2147] According to the invention cited in claim 35, the settlement means can efficiently perform the settlement means.

[2148] According to the invention cited in claim 36, the payment card issuing means can efficiently issue a pay-

ment card.

[2149] According to the invention cited in claim 37, the telephone card issuing means can efficiently issue a telephone card.

[2150] According to the invention cited in claim 38, the ticket issuing means can efficiently issue a ticket.

[2151] According to the invention cited in claim 39, the owner of the electronic wallet purchases, as an electronic payment card, a payment card that is issued by the payment card issuing means, and can download the payment card to the electronic wallet and use it. Thus, the usability is improved.

[2152] According to the invention cited in claim 40, since the owner of the electronic wallet designates the amount of a payment, an illegal act by a store can be prevented.

[2153] According to the invention cited in claim 41, the owner of the electronic wallet can confirm the contents of a trading session, and as a statement of account printed on paper need not be exchanged, a sale can be handled more efficiently.

[2154] According to the invention cited in claim 42, the owner of an electronic wallet can purchase anywhere, as an electronic telephone card, a telephone card that is issued by the telephone card issuing means, and can use the telephone card by downloading it to the electronic wallet. Thus, the usability is improved.

[2155] According to the invention cited in claim 43, a wireless communication service using a payment card clearing method can be received, and the usability is improved.

[2156] According to the invention cited in claim 44, the owner of an electronic wallet can confirm the contents of the wireless communication service that is employed.

[2157] According to the invention cited in claim 45, the owner of an electronic wallet can purchase anywhere, as an electronic ticket, a ticket that is issued by the ticket issuing means, and can use the ticket by downloading it to the electronic wallet. Thus, the usability is improved.

[2158] According to the invention cited in claims 47 and 48, the ticket can be examined accurately and efficiently.

[2159] According to the invention cited in claim 49, since an electronic payment card can be transferred to another person, the usability is improved.

[2160] According to the invention cited in claim 50, an electronic payment card can be precisely transferred and trouble that may accompany the transfer can be prevented.

[2161] According to the invention cited in claim 51, since an electronic telephone card can be transferred to another person, the usability is improved.

[2162] According to the invention cited in claim 52, an electronic telephone card can be precisely transferred and trouble that may accompany the transfer can be prevented.

[2163] According to the invention cited in claim 53, since an electronic ticket can be transferred to another

person, the usability is improved.

[2164] According to the invention cited in claim 54, an electronic ticket can be precisely transferred and trouble that may accompany the transfer can be prevented.

[2165] According to the invention cited in claim 55, the owner of an electronic wallet can install an electronic payment card in the electronic wallet anywhere.

[2166] According to the invention cited in claim 56, an electronic payment card that the owner of the electronic wallet designates can be installed in the electronic wallet anywhere.

[2167] According to the invention cited in claim 57, the owner of the electronic wallet can install an electronic telephone card in the electronic wallet anywhere.

[2168] According to the invention cited in claim 58, an electronic telephone card that the owner of the electronic wallet designates can be installed in the electronic wallet anywhere.

[2169] According to the invention cited in claim 59, the owner of the electronic wallet can install an electronic ticket in the electronic wallet anywhere.

[2170] According to the invention cited in claim 60, an electronic ticket that the owner of the electronic wallet designates can be installed in the electronic wallet anywhere.

[2171] According to the invention cited in claim 61, an illegal installation due to immorality can be prevented.

[2172] According to the invention cited in claim 62, a maximum one hundred million types of electronic payment cards, electronic telephone cards and electronic tickets, and 10 to the 32nd power of cards or tickets of for each type can be identified by simple numerical entry.

[2173] According to the invention cited in claim 63, the owner of the electronic wallet can reduce the communication costs for a purchase, and can also receive, as a gift, an electronic payment card, an electronic telephone card or an electronic ticket. As a result, the distribution and employment of an electronic payment card, an electronic telephone card or an electronic ticket can be accelerated.

[2174] According to the invention cited in claim 64, the distribution and employment of the electronic payment card, the electronic telephone card or the electronic ticket can be accelerated.

[2175] According to the invention cited in claim 65, the contents of a ticket that has been issued can be changed at a low cost.

[2176] According to the invention cited in claim 66, the modification of the contents of an event can be reported to the owner of the electronic ticket, and the electronic ticket can be updated.

[2177] According to the invention cited in claim 67, the owner of the electronic ticket does not have to go to a ticket store for a refund, and can receive the refund anywhere.

[2178] According to the invention cited in claim 68, the calculation function of a computer system can be effi-

ciently distributed to individual information processing means.

[2179] According to the invention cited in claim 69, an electronic payment card to be used and an electronic payment card in the sleeping state can be managed separately, and an efficient service operation is enabled.

[2180] According to the invention cited in claim 70, since an electronic payment card must be registered to be used, even when an unregistered electronic payment card in the sleeping state is stolen, illegal use of that card will not occur.

[2181] According to the invention cited in claim 71, an electronic telephone card to be used and an electronic telephone card in the sleeping state can be managed separately, and an efficient service operation is enabled.

[2182] According to the invention cited in claim 72, since an electronic telephone card must be registered to be used, even when an unregistered electronic telephone card in the sleeping state is stolen, illegal use of that card will not occur.

[2183] According to the invention cited in claim 73, an electronic ticket to be used and an electronic ticket in the sleeping state can be managed separately, and an efficient service operation is enabled.

[2184] According to the invention cited in claim 74, since an electronic ticket must be registered for use, even when an unregistered electronic ticket in the sleeping state is stolen, illegal use of that card will not occur.

[2185] According to the invention cited in claim 75, clearing of the electronic payment card and the transfer of the electronic payment card can be safely performed.

[2186] According to the invention cited in claim 76, the verification process can be mutually performed by the electronic wallet and the electronic payment card clearing means, and the safety of payment card clearing is improved.

[2187] According to the invention cited in claims 78 and 80, various types of electronic payment cards can be safely issued.

[2188] According to the invention cited in claim 79, various types of electronic payment cards can be safely issued by individual payment card issuers.

[2189] According to the invention cited in claim 81, settlement of the communication charge using the electronic telephone card and the transfer of the electronic telephone card can be safely performed.

[2190] According to the invention cited in claim 82, a message generated by the electronic telephone card can be accompanied by the digital signature of the electronic telephone card, and the validity of the message can be verified.

[2191] According to the invention cited in claim 83, the verification process can be mutually performed by the electronic wallet and the electronic telephone card clearing means, and the safety of telephone card clear-

ing is improved.

[2192] According to the invention cited in claims 84 and 86, various types of electronic telephone cards can be safely issued.

5 [2193] According to the invention cited in claim 85, various types of electronic telephone cards can be safely issued by individual telephone card issuers.

[2194] According to the invention cited in claim 87, the examination of an electronic ticket and the transfer of the electronic ticket can be safely performed.

10 [2195] According to the invention cited in claim 88, a message generated by the electronic ticket can be accompanied by the digital signature of the electronic ticket, and the validity of the message can be verified.

15 [2196] According to the invention cited in claim 89, the verification process can be mutually performed by the electronic wallet and the electronic ticket examination means, and the safety of ticket examination is improved.

20 [2197] According to the invention cited in claims 90 and 92, various types of electronic tickets can be safely issued.

[2198] According to the invention cited in claim 91, various types of electronic tickets can be safely issued by individual ticket issuers.

25 [2199] According to the invention cited in claim 93, a payment method can be selected when an electronic payment card is purchased, and the usability is improved.

[2200] According to the invention cited in claim 94, the payment card issuing means can designate a template program that is used for the electronic payment card, and various types of electronic payment cards can be issued.

35 [2201] According to the invention cited in claim 95, the representative component information can be designated when an electronic payment card is issued, and various types of electronic payment cards having a high degree of freedom can be issued.

[2202] According to the invention cited in claim 96, since the signature key of the electronic payment card is updated by registering the card, the safety is improved.

[2203] According to the invention cited in claim 97, an electronic payment card that is to be used can be selected, and the usability is improved.

45 [2204] According to the invention cited in claim 98, since a value that is equal to or greater than the amount of a payment designated by the owner of the electronic wallet is not paid, the safety is improved.

[2205] According to the invention cited in claim 99, since the contents of an electronic payment card used for the payment are precisely represented for the electronic payment card clearing means, the electronic payment card clearing means can determine whether the pertinent electronic payment card is valid.

55 [2206] According to the invention cited in claim 100, the amount of a payment and a person who is to receive the payment are guaranteed, and an illegal charge by a store can be prevented.

[2207] According to the invention cited in claim 101, whether a micro-check is issued by the owner of the electronic payment card is determined, and the validity of the micro-check can be exactly verified.

[2208] According to the invention cited in claim 102, the generation order for a micro-check and the matching of the remaining value can be examined, and further, the validity of the micro-check can be precisely examined.

[2209] According to the invention cited in claim 103, a used micro-check can be automatically collected, and its validity can be examined.

[2210] According to the invention cited in claim 104, the transferring side and the recipient side can negotiate the contents to be transferred.

[2211] According to the invention cited in claim 105, the recipient side can confirm the contents of an electronic payment card to be transferred.

[2212] According to the invention cited in claim 106, since the recipient is guaranteed, even when a payment card transfer certificate message is stolen, the payment card will not be illegally employed.

[2213] According to the invention cited in claim 107, a payment method can be selected when an electronic telephone card is purchased, and the usability is improved.

[2214] According to the invention cited in claim 108, the telephone card issuing means can designate a template program that is used for the electronic telephone card, and various types of electronic telephone cards can be issued.

[2215] According to the invention cited in claim 109, the representative component information can be designated when an electronic telephone card is issued, and various types of electronic telephone cards having a high degree of freedom can be issued.

[2216] According to the invention cited in claim 110, since the signature key of the electronic telephone card is updated by registering the card, the safety is improved.

[2217] According to the invention cited in claim 111, an electronic telephone card that is to be used can be selected, and the usability is improved.

[2218] According to the invention cited in claim 112, the communication service provider can charge a fee in accordance with a wireless communication service that is provided.

[2219] According to the invention cited in claim 113, only a small amount of history information is required, even when the settlement of additional charges is performed many times during a communication session.

[2220] According to the invention cited in claim 114, since the contents of an electronic telephone card used for payment are precisely represented for the electronic telephone card clearing means, the electronic telephone card clearing means can determine whether the pertinent electronic telephone card is valid.

[2221] According to the invention cited in claim 115,

the amount of a payment and a person who is to receive the payment are guaranteed, and an illegal charge by the owner of the electronic telephone card can be prevented.

[2222] According to the invention cited in claim 116, whether a telephone micro-check is issued by the owner of the electronic telephone card is determined, and the validity of the telephone micro-check can be exactly verified.

[2223] According to the invention cited in claim 117, the generation order for a telephone micro-check and the matching of the remaining value can be examined, and the validity of the telephone micro-check can be further precisely examined.

[2224] According to the invention cited in claim 118, a used telephone micro-check can be automatically collected, and the validity can be examined.

[2225] According to the invention cited in claim 119, the transferring side and the recipient side can negotiate the contents to be transferred.

[2226] According to the invention cited in claim 120, the recipient side can confirm the contents of an electronic telephone card that is to be transferred.

[2227] According to the invention cited in claim 121, since the recipient is guaranteed, even when a payment card transfer certificate message is stolen, the payment card will not be illegally employed.

[2228] According to the invention cited in claim 122, a payment method can be selected when an electronic ticket is purchased, and the usability is improved.

[2229] According to the invention cited in claim 123, the ticket issuing means can designate a template program that is used for the electronic ticket, and various types of electronic tickets can be issued.

[2230] According to the invention cited in claim 124, the representative component information can be designated when an electronic ticket is issued, and various types of electronic tickets having a high degree of freedom can be issued.

[2231] According to the invention cited in claim 125, since the signature key of the electronic ticket is updated by registering the ticket, the safety is improved.

[2232] According to the invention cited in claim 126, an electronic ticket that is to be used can be selected, and the usability is improved.

[2233] According to the invention cited in claim 127, the electronic ticket examination means can perform the examination process in accordance with a ticket that is presented.

[2234] According to the invention cited in claim 128, since the contents of an electronic ticket to be used are precisely represented for the electronic ticket examination means, the electronic ticket examination means can determine whether the pertinent electronic ticket is valid.

[2235] According to the invention cited in claim 129, the contents of the electronic ticket that is examined is guaranteed, and an illegal charge by the owner of the

electronic ticket can be prevented.

[2236] According to the invention cited in claim 130, whether a ticket examination response message is issued by the owner of the electronic ticket is determined, and the validity of the ticket examination response can be exactly verified.

[2237] According to the invention cited in claim 131, the generation order for a ticket examination response message and the matching of the changes of the statuses can be examined, and the validity of the ticket examination response message can be precisely examined.

[2238] According to the invention cited in claim 132, a ticket examination response can be automatically collected, and the validity can be examined.

[2239] According to the invention cited in claim 133, the transferring side and the recipient side can negotiate the contents to be transferred.

[2240] According to the invention cited in claim 134, the recipient side can confirm the contents of an electronic ticket that is to be transferred.

[2241] According to the invention cited in claim 135, since the recipient is guaranteed, even when a ticket transfer certificate message is stolen, the ticket will not be illegally employed.

[2242] According to the invention cited in claim 136, the payment card issuer, the telephone card issuer and the ticket issuer can designate the procedures for clearing.

[2243] According to the invention cited in claim 137, an electronic payment card, an electronic telephone card and an electronic ticket can be issued without keeping a purchaser waiting.

[2244] According to the invention cited in claim 138, an electronic payment card, an electronic telephone card and an electronic ticket can be issued without keeping a purchaser waiting.

[2245] According to the invention cited in claim 139, a plurality of electronic payment cards, electronic telephone cards and electronic tickets, and history information can also be managed in the memory of an electronic wallet that has a limited capability.

[2246] According to the invention cited in claim 140 and 141, the service life of a battery for the electronic wallet or for the electronic payment card clearing means can be extended.

[2247] According to the invention cited in claim 144, the counterfeiting of printed material can be prevented. Further, according to the invention for a recording medium on which are stored various programs, such as a control program for the central processing unit of the electronic wallet, these programs can be distributed in a portable form.

[2248] According to the invention cited in claim 155, the third storage means for storing the identification information and authorization information for a user is loaded into an arbitrary electronic wallet, so that the electronic wallet can be used as the electronic wallet of

that user.

[2249] According to the invention cited in claim 156, communication with the service providing means is not required when the third storage means is to be loaded into and unloaded from the electronic wallet.

[2250] According to the invention cited in claim 157, an electronic negotiable card that is obtained using the electronic wallet can be carried while stored in the IC card.

[2251] According to the invention of printed material on which is printed electronic payment installation information, electronic telephone card installation information or electronic ticket installation information, and a recording medium on which such information is stored, an electronic payment card, an electronic telephone card or an electronic ticket can be transmitted along a distribution route.

[2252] The printed material to which the removable coating is applied can be prevent the leakage of installation information before this printed material is purchased.

Claims

1. A mobile electronic commerce system for paying, via wireless communication means, a required amount from an electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, comprising:

service means for connecting said electronic wallet and said supply side via said communication means,

wherein said service means installs, via said communication means, a program for an electronic negotiable card in said electronic wallet; wherein said electronic negotiable card that is installed is employed to receive a product or a service, or a required permission, from said supply side;

wherein based on a program for said electronic negotiable card a settlement process for which said electronic negotiable card is used, is performed by said electronic wallet and said supply side via said communication means; and wherein, in association with said settlement process, said data that are stored in said electronic wallet and at said supply side are transmitted to said service means at a predetermined time, and are managed thereat.

2. A mobile electronic commerce system for paying, via wireless communication means, a required amount using an electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side,

- wherein, via said wireless communication means, said electronic wallet applies the purchase of a program for an electronic negotiable card to service means for issuing said program for said electronic negotiable card; 5
- wherein said service means receives from electronic negotiable card issuing means data concerning said electronic negotiable card, and with settlement means performs a settlement that is associated with the purchase of said electronic negotiable card; 10
- wherein, via said wireless communication means, said program for said electronic negotiable card is installed in said electronic wallet;
- wherein said electronic negotiable card that is installed is employed for receiving a product or a service, or a required permission, from said supply side; and 15
- wherein, based on said program for said negotiable card, a settlement process based on the use of said negotiable card is performed by said electronic wallet and said supply side via said communication means. 20
3. A mobile electronic commerce system according to claim 1 or 2, wherein, in said settlement process for which said negotiable card is used, said electronic wallet generates an electronic check corresponding to a payment amount based on said program provided for said negotiable card, and transmits said electronic check to said supply side via said wireless communication means; wherein said supply side, upon receiving said electronic check, transmits an electronic receipt to said electronic wallet; wherein, thereafter, said electronic wallet and said supply side respectively store said electronic receipt and said electronic check as data concerning said settlement process. 25 30 35
 4. A mobile electronic commerce system according to claim 1 or 2, wherein, in said settlement process for which said electronic negotiable card is used, based on said program provided for said electronic negotiable card said electronic wallet transmits data for said electronic negotiable card to said supply side via said wireless communication means; wherein said supply side, upon receiving said data for said electronic negotiable card, transmits to said electronic wallet an electronic certificate required for the granting of entrance permission and the admission of the owner of said electronic wallet; and wherein, thereafter, said electronic wallet and said supply side respectively store said electronic certificate and said data for said electronic negotiable card as data concerning said settlement process. 40 45 50 55
 5. A mobile electronic commerce system according to claim 1 or 2, wherein, in order to transfer said electronic negotiable card that is installed in said electronic wallet to a different electronic wallet, said electronic wallet generates a transfer message using said electronic negotiable card and transmits said message to said different electronic wallet; wherein said electronic wallet deletes said stored electronic negotiable card, and said different electronic wallet transmits, to said service means, said transfer message for said negotiable card; wherein, thereafter, said service means installs a program for said electronic negotiable card in said different electronic wallet.
 6. A mobile electronic commerce system according to claim 1 or 2, wherein said electronic wallet transmits to said service means, via said wireless communication means, an installation number to be recorded on or in a distribution medium, such as printed matter or a recording medium; and wherein said service means receives, from negotiable card issuing means, data concerning an electronic negotiable card that is to be issued, and through wireless communication installs a program for an electronic negotiable card corresponding to said installation number.
 7. A mobile electronic commerce system according to claim 1 or 2, wherein said service means manages a template program that is a model of a program for an electronic negotiable card, and based on said template program generates said program for said electronic negotiable card and installs said program in said electronic wallet.
 8. A mobile electronic commerce system for paying, via wireless communication means, a required amount from an electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, wherein a program for an electronic negotiable card includes an inherent private key, and wherein, when an electronic wallet employs said negotiable card, said private key is employed to add a digital signature to data that are to be transmitted to a supply side via communication means.
 9. A mobile electronic commerce system for paying, via wireless communication means, a required amount from an electronic wallet that includes said wireless communication means, and for receiving a product or a service, or a required permission, from a supply side, wherein said electronic wallet holds an electronic payment card that serves as an electronic payment card program, and employs said electronic payment card when paying said required amount for

said product or said service that is received from said supply side; and
 wherein, via said wireless communication means, said electronic wallet and said supply side perform a settlement process that is associated with said payment.

10. A mobile electronic commerce system according to claim 9, wherein an electronic payment card settlement means for making a payment using said electronic payment card is provided for said supply side.
11. A mobile electronic commerce system according to claim 10, wherein service means is provided to connect, via said communication means, said electronic wallet and said electronic payment card settlement means and to connect, via said communication means, said payment card issuing means and said settlement means, so that said electronic wallet can purchase said electronic payment card through said service means.
12. A mobile electronic commerce system according to claim 11, wherein said electronic wallet, said electronic payment card settlement means, and said service means individually include a plurality of types of communication means, and wherein said electronic wallet, said electronic payment card settlement means, and said service means employ different communication means when communication among the three is conducted.
13. A mobile electronic commerce system for paying, via wireless communication means, a required amount from an electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, wherein said electronic wallet holds an electronic telephone card that serves as an electronic telephone card program, and employs said electronic telephone card when paying a required amount for a communication that is performed via wireless communication means using an exchange service provided by said supply side; and wherein said electronic wallet and said supply side perform, via said wireless communication means, a settlement process that accompanies said payment.
14. A mobile electronic commerce system according to claim 13, wherein said supply side includes communication line exchange means and electronic telephone card settlement means for settling said payment using said electronic telephone card.
15. A mobile electronic commerce system according to claim 14, wherein service means is provided for

connecting, via said communication means, said electronic wallet and said electronic payment card settlement means, and for connecting, via said communication means, said payment card issuing means and said settlement means, so that said electronic wallet can purchase said electronic telephone card through said service means.

16. A mobile electronic commerce system according to claim 15, wherein said electronic wallet, said electronic telephone card settlement means, and said service means individually include a plurality of types of communication means, and wherein said electronic wallet, said electronic telephone card settlement means, and said service means employ different communication means when communication among the three is conducted.
17. A mobile electronic commerce system for paying, via wireless communication means, a required amount from an electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, wherein said electronic wallet holds an electronic ticket that is electronically constituted, and provides information concerning said electronic ticket; and wherein said electronic wallet and said supply side perform, via said wireless communication means, an examination process for said electronic ticket for granting permission for an admission.
18. A mobile electronic commerce system according to claim 17, wherein electronic ticket examination means for examining said electronic ticket is provided for said supply side.
19. A mobile electronic commerce system according to claim 18, wherein service means is provided for connecting, via said communication means, said electronic wallet and said electronic ticket examination means, and for connecting, via said communication means, said ticket issuing means and said settlement means, so that said electronic wallet can purchase said electronic ticket through said service means.
20. A mobile electronic commerce system according to claim 18, wherein said electronic wallet, said electronic ticket examination means, and said service means individually include a plurality of types of communication means, and wherein said electronic wallet, said electronic ticket examination means, and said service means employ different communication means when communication among the three is performed.
21. A mobile electronic commerce system comprising:

- said electronic wallet defined in claim 9;
 electronic payment card settlement means;
 electronic telephone card settlement means;
 electronic ticket examination means;
 service provision means; 5
 settlement processing means;
 payment card issuing means;
 telephone card issuing means; and
 ticket issuing means. 10
22. A mobile electronic commerce system according to claim 11, wherein said electronic wallet holds an electronic credit card and employs said electronic credit card to purchase said electronic payment card, said electronic telephone card or said electronic ticket. 15
23. A mobile electronic commerce system according to claim 12, wherein said electronic wallet includes a plurality of kinds of wireless communication means as said plurality of types of communication means. 20
24. A mobile electronic commerce system according to claim 23, wherein, as means for engaging in wireless communication with said electronic payment card settlement means or said electronic ticket examination means, said electronic wallet includes wireless communication means that has a shorter communication distance and a higher directivity than has the wireless communication means employed for said electronic telephone card settlement or for said service providing means. 25 30
25. A mobile electronic commerce system according to claim 24, wherein, as means for engaging in wireless communication with said electronic payment card settlement means or said electronic ticket examination means, said electronic wallet includes optical communication means and radio communication means for engaging in wireless communication with said electronic telephone card settlement means or said service providing means. 35 40
26. A mobile electronic commerce system according to claim 10, wherein said electronic payment card settlement means includes wireless communication means for engaging in communication with said service providing means. 45
27. A mobile electronic commerce system according to claim 10, wherein said electronic payment card settlement means is an automatic vending machine that includes automatic product or service providing means. 50
28. A mobile electronic commerce system according to claim 9, wherein said electronic wallet comprises: 55
- input means for entering a numerical value and for performing a selection operation;
 a central processing unit for generating data to be transmitted via said wireless communication means, and for processing data received via said wireless communication means;
 first storage means for storing a control program for controlling an operation performed by said central processing unit;
 display means for displaying data processed by said central processing unit; and
 second storage means for storing said data processed by said central processing unit, wherein said electronic ticket, said electronic payment card or said electronic telephone card is stored in said second storage means.
29. A mobile electronic commerce system according to claim 10, wherein said electronic payment card settlement means includes:
 optical communication means for communicating with said electronic wallet;
 communication means for communicating with said service providing means;
 input means for entering a numerical value and performing a selection operation;
 a central processing unit for generating data to be transmitted via said optical communication means and said communication means, and for processing data received via said optical communication means and said communication means;
 first storage means for storing a control program for controlling an operation performed by said central processing unit;
 display means for displaying data processed by said central processing unit; and
 second storage means for storing said data processed by said central processing unit, wherein a settlement process program module for said electronic payment card is stored in said second storage means.
30. A mobile electronic commerce system according to claim 10, wherein said electronic payment card settlement means comprises:
 optical communication means for communicating with said electronic wallet;
 radio communication means for communicating with said service providing means;
 product identification means for identifying a product type;
 input means for entering a numerical value and for performing a selection operation;
 a central processing unit for calculating a charge for said product, for generating data to

be transmitted via said optical communication means and said radio communication means, and for processing data received via said optical communication means and said radio communication means;

5

first storage means for storing a control program for controlling an operation performed by said central processing unit;

display means for displaying data processed by said central processing unit;

10

second storage means for storing said data processed by said central processing unit; and third storage means for storing value information for said product,

wherein a settlement process program module for said electronic payment card is stored in said second storage means.

15

31. A mobile electronic commerce system according to claim 27, wherein said automatic vending machine comprises:

20

optical communication means for communicating with said electronic wallet;

radio communication means for communicating with said service providing means;

25

selection means for selecting a product to be purchased or a service;

automatic providing means for providing said product or said service;

30

a central processing unit for generating data to be transmitted via said optical communication means and said radio communication means, and for processing data received via said optical communication means and said radio communication means;

35

first storage means for storing a control program for controlling an operation performed by said central processing unit;

display means for displaying data processed by said central processing unit;

40

second storage means for storing said data processed by said central processing unit;

third storage means for storing value information and stock information for said product; and

45

fourth storage means for storing promotion information for said product or for said service, wherein a settlement process program module for said electronic payment card is stored in said second storage means.

50

32. A mobile electronic commerce system according to claim 14 or 21, wherein said electronic telephone card settlement means comprises:

55

radio communication means for communicating with said electronic wallet;

communication means for communicating with

said service providing means;

communication line exchange means for exchanging a plurality of communication lines;

a central processing unit for generating data to be transmitted via said radio communication means and said communication means, and for

processing data received via said radio communication means and said communication means;

first storage means for storing a control program for controlling an operation performed by said central processing unit; and

second storage means for storing said data processed by said central processing unit,

wherein a settlement process program module for said electronic telephone card is stored in said second storage means.

33. A mobile electronic commerce system according to claim 17, wherein said electronic ticket examination means comprises:

optical communication means for communicating with said electronic wallet;

communication means for communicating with said service providing means;

input means for entering a numerical value and for performing a selection operation;

a central processing unit for generating data to be transmitted via said optical communication means and said communication means, and for processing data received via said optical communication means and said communication means;

first storage means for storing a control program for controlling an operation performed by said central processing unit;

display means for displaying data processed by said central processing unit; and

second storage means for storing said data processed by said central processing unit,

wherein an examination program module for said electronic ticket is stored in said second storage means.

34. A mobile electronic commerce system according to claim 21, wherein said service providing means comprises:

user information storage means for storing information concerning said electronic wallet and information concerning a settlement contract concluded with an owner of said electronic wallet;

merchant information storage means for storing information concerning said electronic payment card settlement means, said electronic telephone card settlement means and said

electronic ticket examination means, and information concerning a settlement contracts concluded with owners of electronic payment cards, electronic telephone cards and electronic tickets;

5

settlement processor information storage means for storing information concerning said settlement processing means;

payment card issuer information storage means for storing information concerning said payment card issuing means, and information concerning a settlement contract concluded with an owner of said payment card issuing means;

10

telephone card issuer information storage means for storing information concerning said telephone card issuing means, and information concerning a settlement contract concluded with an owner of said telephone card issuing means;

15

20

ticket issuer information storage means for storing information concerning said ticket issuing means, and information concerning a settlement contract concluded with an owner of said ticket issuing means;

25

service director information storage means for storing list information for said electronic wallet, said electronic payment card settlement means, said electronic telephone card settlement means, said electronic ticket examination means, said settlement processing means, said payment card issuing means, said telephone card issuing means and said ticket issuing means, and information concerning said electronic ticket, said electronic payment card and said electronic telephone card; and a computer system for processing data in a service provision process for selling, issuing and managing said electronic ticket, said electronic payment card and said electronic telephone card.

30

35

40

35. A mobile electronic commerce system according to claim 11, wherein said settlement processing means comprises:

45

communication means for communicating with said service providing means;
subscriber information storage means for storing information concerning a settlement contract concluded with an owner of said electronic wallet;
member shop information storage means for storing information concerning settlement contracts concluded with owners of electronic payment card settlement means, electronic telephone card settlement means, electronic ticket examination means, payment card issu-

50

55

ing means, telephone card issuing means, and ticket issuing means; and

a computer system for processing data employed in a settlement process.

36. A mobile electronic commerce system according to claim 11, wherein said payment card issuing means comprises:

communication means for communicating with said service providing means;

customer information storage means for storing information concerning the purchase history of a customer;

payment card issuance information storage means for storing information concerning a payment card that has been issued;

payment card information storage means for storing information concerning the stock of payment cards; and

a computer system for processing data during a payment card issuing transaction process.

37. A mobile electronic commerce system according to claim 15, wherein said telephone card issuing means comprises:

communication means for communicating with said service providing means;

customer information storage means for storing information concerning the purchase history of a customer;

telephone card issuance information storage means for storing information concerning a telephone card that has been issued;

telephone card information storage means for storing information concerning the stock of telephone cards; and

a computer system for processing data concerning a telephone card issuing transaction process.

38. A mobile electronic commerce system according to claim 19, wherein said ticket issuing means comprises:

communication means for communicating with said service providing means;

customer information storage means for storing information concerning the purchase history of a customer;

ticket issuance information storage means for storing information concerning a ticket that has been issued;

ticket information storage means for storing information concerning the stock of tickets; and a computer system for processing data concerning a ticket issuing transaction process.

39. A mobile electronic commerce system according to claim 11, wherein said electronic wallet generates and then transmits, to said service providing means, a payment card application message for the purchase of an electronic payment card; wherein said service providing means, upon receiving said payment card application message, communicates with said payment card issuing means and receives therefrom an electronic payment card issuance request message requesting that said service providing means perform an electronic payment card issuing process and an electronic payment card charge settlement process; wherein said service providing means, upon receiving said request message, communicates with said settlement processing means to perform the settlement process for the charge for said payment card, generates an electronic payment card from payment card information that is generated by said payment card issuing means and is included in said electronic payment card issuance request message, and transmits said electronic payment card to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic payment card, stores said electronic payment card in said second storage means thereof.
40. A mobile electronic commerce system according to claim 28, wherein a micro-check message, generated by an electronic payment card stored in said second storage means, is transmitted to said electronic payment card settlement means in order to confirm the submission of a payment that is the equivalent of an amount entered by said input means.
41. A mobile electronic commerce system according to claim 40, wherein said electronic payment card settlement means, upon receiving said micro-check message, generates and then transmits, to said electronic wallet, said reception message to acknowledge that said micro-check message has been received.
42. A mobile electronic commerce system according to claim 15, wherein said electronic wallet generates and then transmits, to said service providing means, a telephone card application message requesting the purchase of an electronic telephone card; wherein said service providing means, upon receiving said telephone card application message, communicates with said telephone card issuing means and receives therefrom an electronic telephone card issuance request message indicating said service providing means has been requested to perform an electronic telephone card issuing process and an electronic telephone card charge settlement process; wherein said service providing means, upon receiving said request message, communicates with said settlement processing means to perform the settlement for the charge for said telephone card, generates an electronic telephone card using telephone card information that is generated by said telephone card issuing means and is included in said electronic telephone card issuance request message, and transmits said electronic telephone card to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic telephone card, stores said electronic telephone card in said second storage means thereof.
43. A mobile electronic commerce system according to claim 28, wherein a telephone micro-check message is generated by an electronic telephone card stored in said second storage means and is transmitted to said electronic telephone card settlement means in order to confirm the submission of a payment that is equivalent to an amount charged by said electronic telephone settlement means.
44. A mobile electronic commerce system according to claim 43, wherein said electronic telephone card settlement means, upon receiving said telephone micro-check message, generates and then transmits, to said electronic wallet, a receipt message acknowledging that said telephone micro-check message has been received.
45. A mobile electronic commerce system according to claim 19, wherein said electronic wallet generates and then transmits, to said service providing means, a ticket application message requesting the purchase of an electronic ticket; wherein said service providing means, upon receiving said ticket application message, communicates with said ticket issuing means, and receives therefrom an electronic ticket issuance request message that indicates said service providing means has been requested to perform an electronic ticket issuing process and an electronic ticket charge settlement process; wherein said service providing means, upon receiving said request message, communicates with said settlement processing means to perform the settlement of the charge for said ticket, generates an electronic ticket from ticket information that is generated by said ticket issuing means and is included in said electronic ticket issuance request message, and transmits said electronic ticket to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic ticket stores said electronic ticket in said second storage means thereof.
46. A mobile electronic commerce system according to claim 28, wherein said electronic wallet generates a

ticket presenting message that describes the contents of said electronic ticket stored in said second storage means, and transmits said ticket presenting message to said electronic ticket examination means.

47. A mobile electronic commerce system according to claim 28, wherein said electronic wallet, upon receiving a command message from said electronic ticket examination means, changes said electronic ticket to a post-examined state, and generates and then transmits, to said electronic ticket examination means, a ticket examination response message that describes the contents of said electronic ticket that has been changed.

48. A mobile electronic commerce system according to claim 47, wherein said electronic ticket examination means, upon receiving said ticket examination response message, generates and then transmits, to said electronic wallet, an examination certificate message that verifies said electronic ticket has been examined.

49. A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates a payment card transfer certificate message verifying that said electronic payment card stored in said second storage means is to be transferred to a second electronic wallet, and transmits said payment card transfer certificate message via wireless communication means to said second electronic wallet; wherein said second electronic wallet transmits, to said service providing means, said payment card transfer certificate message that is received; wherein said service providing means performs an examination to establish the validity of said payment card transfer certificate message that is received, and transmits, to said second electronic wallet, the electronic payment card that is described in said payment card transfer certificate message; and wherein said second electronic wallet stores, in said second storage means thereof, said electronic payment card that is received.

50. A mobile electronic commerce system according to claim 49, wherein said second electronic wallet, upon receiving said payment card transfer certificate message, generates a payment card receipt message confirming that said payment card transfer certificate message has been received, and transmits said payment card receipt message via said wireless communication means to said first electronic wallet; and wherein said first electronic wallet, upon receiving said payment card receipt message, deletes said electronic payment card stored in said second storage means thereof.

51. A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates a telephone card transfer certificate message confirming that said electronic telephone card stored in said second storage means is to be transferred to a second electronic wallet, and transmits said telephone card transfer certificate message via wireless communication means to said second electronic wallet; wherein said second electronic wallet transmits, to said service providing means, said telephone card transfer certificate message that is received; wherein said service providing means performs an examination to establish the validity of said telephone card transfer certificate message that is received, and transmits, to said second electronic wallet, the electronic telephone card that is described in said telephone card transfer certificate message; and wherein said second electronic wallet stores, in said second storage means thereof, said electronic telephone card that is received.

52. A mobile electronic commerce system according to claim 28, wherein said second electronic wallet, upon receiving said telephone card transfer certificate message, generates a telephone card receipt message confirming that said telephone card transfer certificate message has been received, and transmits said telephone card receipt message via said wireless communication means to said first electronic wallet; and wherein said first electronic wallet, upon receiving said telephone card receipt message, deletes said electronic telephone card stored in said second storage means thereof.

53. A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates a ticket transfer certificate message confirming that said electronic ticket stored in said second storage means is to be transferred to a second electronic wallet, and transmits said ticket transfer certificate message via wireless communication means to said second electronic wallet; wherein said second electronic wallet transmits, to said service providing means, said ticket transfer certificate message that is received; wherein said service providing means performs an examination to establish the validity of said ticket transfer certificate message that is received, and transmits, to said second electronic wallet, an electronic ticket that is described in said ticket transfer certificate message; and wherein said second electronic wallet stores, in said second storage means thereof, said electronic ticket that is received.

54. A mobile electronic commerce system according to claim 53, wherein said second electronic wallet, upon receiving said ticket transfer certificate mes-

sage, generates a ticket receipt message confirming that said ticket transfer certificate message has been received, and transmits said ticket receipt message via said wireless communication means to said first electronic wallet; and wherein said first electronic wallet, upon receiving said ticket receipt message, deletes said electronic ticket stored in said second storage means thereof.

55. A mobile electronic commerce system according to claim 11, wherein said electronic wallet generates and then transmits, to said service providing means, an electronic payment card installation request message requesting the installation of an electronic payment card; wherein said service providing means, upon receiving said payment card installation request message, communicates with said payment card issuing means and receives therefrom an electronic payment card installation request message indicating that said service providing means is requested to install an electronic payment card; wherein said service providing means, upon receiving said request message, generates an electronic payment card using payment card information that is generated by said payment card issuing means and is included in said electronic payment card installation request message, and transmits said electronic payment card to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic payment card stores said electronic payment card in said second storage means thereof.
56. A mobile electronic commerce system according to claim 55, wherein said electronic payment card installation request message includes electronic payment card installation information that is entered by input means for said electronic wallet and that uniquely describes an electronic payment card that is to be installed.
57. A mobile electronic commerce system according to claim 15, wherein said electronic wallet generates and then transmits, to said service providing means, an electronic telephone card installation request message for requesting the installation of an electronic telephone card; wherein said service providing means, upon receiving said telephone card installation request message, communicates with said telephone card issuing means, and receives therefrom an electronic telephone card installation request message indicating that said service providing means is to install an electronic telephone card; wherein said service providing means, upon receiving said request message, generates an electronic telephone card using telephone card information that is generated by said telephone card issuing means and that is included

in said electronic telephone card installation request message, and transmits said electronic telephone card to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic telephone card, stores said electronic telephone card in said second storage means thereof.

58. A mobile electronic commerce system according to claim 57, wherein said electronic telephone card installation request message includes said electronic telephone card installation information that is entered by input means for said electronic wallet and that uniquely describes an electronic telephone card that is to be installed.
59. A mobile electronic commerce system according to claim 19, wherein said electronic wallet generates and then transmits, to said service providing means, an electronic ticket installation request message requesting the installation of an electronic ticket; wherein said service providing means, upon receiving said ticket installation request message, communicates with said ticket issuing means, and receives therefrom an electronic ticket installation request message indicating that said service providing means is to install an electronic ticket; wherein said service providing means, upon receiving said request message, generates an electronic ticket using ticket information that is generated by said ticket issuing means and is included in said electronic ticket installation request message, and transmits said electronic ticket to said electronic wallet; and wherein said electronic wallet, upon receiving said electronic ticket, stores said electronic ticket in said second storage means thereof.
60. A mobile electronic commerce system according to claim 59, wherein said electronic ticket installation request message includes said electronic ticket installation information that is entered by input means for said electronic wallet and that uniquely describes an electronic ticket that is to be installed.
61. A mobile electronic commerce system according to claim 55, wherein said electronic payment card installation information, said electronic telephone card installation information or said electronic ticket installation information consists of first identification information describing a type of electronic payment card, a type of electronic telephone card or a type of electronic ticket, and second identification information that uniquely describes an electronic payment card, an electronic telephone card or an electronic ticket, of a type described using said first identification information, that is to be installed; and wherein said second identification information is information generated at random.

62. A mobile electronic commerce system according to claim 61, wherein said first identification information and said second identification information are represented by 8-digit numerals and 32-digit numerals. 5
63. A mobile electronic commerce system according to claim 55, wherein an object whereon or wherein said electronic payment card installation information, said electronic telephone installation information or said electronic ticket installation information is printed or engraved is employed as sales distribution means or transfer means for said electronic payment card, said electronic telephone card or said electronic ticket. 10
64. A mobile electronic commerce system according to claim 55, wherein a recording medium on which said electronic payment card installation information, said electronic telephone installation information or said electronic ticket installation information is stored is employed as sales distribution means or transfer means for an electronic payment card, an electronic telephone card or an electronic ticket. 15
65. A mobile electronic commerce system according to claim 28, wherein said service providing means generates and then transmits, to said electronic wallet, a modification command message for the modification of the contents of said electronic ticket; and said electronic wallet, upon receiving said modification command message, updates said electronic ticket stored in said second storage means to provide a new electronic ticket as is described in said modification command message. 20 25 30
66. A mobile electronic commerce system according to claim 28, wherein said service providing means generates and then transmits, to said electronic wallet, a modification notification message for the modification of the contents of said electronic ticket; wherein said electronic wallet, upon receiving said modification notification message, generates and then transmits, to said service providing means, a reaction selection message acknowledging receipt of the message for the modification of said contents of said electronic ticket; wherein said service providing means, upon receiving said reaction selection message, generates and then transmits, to said electronic wallet, a modification command message instructing the modification of said contents of said electronic ticket; and wherein said electronic wallet, upon receiving said modification command message, updates said electronic ticket stored in said second storage means to provide a new electronic ticket that is described in said modification command message. 35 40 45 50 55
67. A mobile electronic commerce system according to claim 28, wherein said service providing means generates and then transmits, to said electronic wallet, a modification notification message for the modification of the contents of said electronic ticket; wherein said electronic wallet, upon receiving said modification notification message, generates and then transmits, to said service providing means, a reaction selection message requesting a refund for said electronic ticket; wherein said service providing means, upon receiving said reaction selection message, communicates with said settlement processing means to issue a refund for said electronic ticket, and generates and then transmits, to said electronic wallet, a refund receipt message indicating that a refund process has been completed; and wherein said electronic wallet, upon receiving said refund receipt message, deletes said electronic ticket from said second storage means.
68. A mobile electronic commerce system according to claim 21, wherein a computer system in said service providing means comprises:
- user information processing means for communicating with said electronic wallet and for processing information stored in user information storage means;
- merchant information processing means for communicating with said electronic payment card settlement means, said electronic telephone card settlement means or said electronic ticket examination means, and for processing information stored in merchant information storage means;
- settlement processor information processing means for communicating with said electronic settlement processing means, and for processing information stored in settlement processor information storage means;
- payment card issuer information processing means for communicating with said payment card issuing means, and for processing information stored in payment card issuer information storage means;
- telephone card issuer information processing means for communicating with said telephone card issuing means, and for processing information stored in telephone card issuer information storage means;
- ticket issuer information processing means for communicating with said ticket issuing means, and for processing information stored in ticket issuer information storage means;
- service director information processing means for communicating with said user information processing means, said merchant information processing means, said settlement processor information processing means, said payment

card issuer information processing means, said telephone card issuer information processing means and said ticket issuer information processing means, and for interacting with those means while processing data during a service providing process; and

service manager information processing means for controlling the generation and the deletion of said user information processing means, said merchant information processing means, said settlement processor information processing means, said payment card issuer information processing means, said telephone card issuer information processing means, said ticket issuer information processing means and said service director information processing means.

69. A mobile electronic commerce system according to claim 34, wherein said electronic wallet generates and then transmits, to said service providing means, a payment card registration request message requesting that said service providing means register, as an electronic payment card that is to be used by the owner of said electronic wallet, an electronic payment card that is stored in said second storage means; and wherein said service providing means, upon receiving said payment card registration request message, registers said electronic payment card for use in said service director information storage means.

70. A mobile electronic commerce system according to claim 69, wherein said service providing means, upon receiving said payment card registration request message, generates and then transmits, to said electronic wallet, a registered card certificate confirming that said electronic payment card has been registered for use; and wherein said electronic wallet stores, in said second storage means, said registered card certificate that is received and changes the state of said electronic payment card to the usable state.

71. A mobile electronic commerce system according to claim 34, wherein said electronic wallet generates and then transmits, to said service providing means, a telephone card registration request message requesting that service providing means register, as an electronic telephone card that is to be used by the owner of said electronic wallet, an electronic telephone card that is stored in said second storage means; and wherein said service providing means, upon receiving said telephone card registration request message, registers said electronic telephone card for use in said service director information storage means.

72. A mobile electronic commerce system according to claim 71, wherein said service providing means, upon receiving said telephone card registration request message, generates and then transmits, to said electronic wallet, a registered card certificate confirming that said electronic telephone card has been registered for use; and wherein said electronic wallet stores, in said second storage means, said registered card certificate that is received and changes the state of said electronic telephone card to the usable state.

73. A mobile electronic commerce system according to claim 34, wherein said electronic wallet generates and then transmits, to said service providing means, a ticket registration request message requesting that said second storage means register, as an electronic ticket that is to be used by the owner of said electronic wallet, an electronic ticket that is stored in said second storage means; and wherein said service providing means, upon receiving said ticket registration request message, registers said electronic ticket for use in said service director information storage means.

74. A mobile electronic commerce system according to claim 73, wherein said service providing means, upon receiving said ticket registration request message, generates and then transmits, to said electronic wallet, a registered ticket certificate that verifies said electronic ticket has been registered for use; and wherein said electronic wallet stores, in said second storage means, said registered ticket certificate that is received, and changes the state of said electronic ticket to the usable state.

75. A mobile electronic commerce system according to claim 28, wherein said electronic payment card comprises:

a payment card program;
presented card information describing the contents of said electronic payment card when issued; and

a card certificate indicating that said electronic payment card is authentic. Said payment card program includes:

electronic payment card state management information; and

payment card program data for specifying an operation to be performed by said electronic payment card. The digital signature of the owner of said service providing means is provided for said presented card information.

76. A mobile electronic commerce system according to claim 75, wherein said payment card program includes a card signature private key that is

employed for a digital signature provided for said electronic payment card, and wherein said card certificate is a public key certificate verifying that a card signature public key that is paired with said card signature private key is authentic.

77. A mobile electronic commerce system according to claim 75, wherein a settlement program module for said electronic payment card includes two cryptographic keys, an accounting device authentication private key and a card authentication public key, and wherein said payment card program includes an accounting device authentication public key, which is paired with said accounting device authentication private key, and a card authentication private key, which is paired with said card authentication public key.

78. A mobile electronic commerce system according to claim 75, wherein said payment card program data includes:

a transaction module program for specifying the procedures to be used for message data that are exchanged by said electronic wallet and said electronic payment card settlement means;
a display module program for specifying the manner in which said electronic payment card is to be displayed; and
representative component information for said electronic payment card,
wherein a central processing unit in said electronic wallet processes, in accordance with said transaction module program for said electronic payment card, said message data that are exchanged with said electronic payment card settlement means, and displays said representative component information in accordance with said display module program of said electronic payment card, so that on display means said electronic payment card is displayed in said electronic wallet.

79. A mobile electronic commerce system according to claim 34, wherein a template program that constitutes a model for said electronic payment card is stored in said payment card issuer information storage means for said service providing means.

80. A mobile electronic commerce system according to claim 79, wherein said template program for said electronic payment card includes:

a transaction module program for said electronic payment card;
a display module program; and
representative component information.

Therefore, various types of electronic payment cards can be safely issued.

81. A mobile electronic commerce system according to claim 28, wherein said electronic telephone card comprises:

a telephone card program;
presented card information describing the contents of said electronic telephone card when issued; and
a card certificate indicating that said electronic telephone card is authentic,
wherein said telephone card program includes: electronic telephone card state management information; and
telephone card program data for specifying an operation to be performed by said electronic telephone card, and
wherein the digital signature of the owner of said service providing means is provided for said presented card information.

82. A mobile electronic commerce system according to claim 81, wherein said telephone card program includes a card signature private key that is employed for a digital signature provided for said electronic telephone card, and wherein said card certificate is a public key certificate verifying that a card signature public key that is paired with said card signature private key is authentic.

83. A mobile electronic commerce system according to claim 81, wherein a settlement program module for said electronic telephone card includes two cryptographic keys, an accounting device authentication private key and a card authentication public key, and wherein said telephone card program includes an accounting device authentication public key, which is paired with said accounting device authentication private key, and a card authentication private key, which is paired with said card authentication public key.

84. A mobile electronic commerce system according to claim 81, wherein said telephone card program data includes:

a transaction module program for specifying the procedures to be used for message data that are exchanged by said electronic wallet and said electronic telephone card settlement means;
a display module program for specifying the manner in which said electronic telephone card is to be displayed; and
representative component information for said electronic telephone card, and

wherein a central processing unit in said electronic wallet processes, in accordance with said transaction module program for said electronic telephone card, said message data that are exchanged with said electronic telephone card settlement means, and displays said representative component information in accordance with said display module program for said electronic telephone card, so that on display means said electronic telephone card is displayed in said electronic wallet.

85. A mobile electronic commerce system according to claim 34, wherein a template program that constitutes a model for said electronic telephone card is stored in said telephone card issuer information storage means for said service providing means.

86. A mobile electronic commerce system according to claim 85, wherein said template program for said electronic telephone card includes:

a transaction module program for said electronic telephone card;
a display module program; and
representative component information.

87. A mobile electronic commerce system according to claim 28, wherein said electronic ticket comprises:

a ticket program;
presented ticket information describing the contents of said electronic ticket when issued; and
a ticket certificate indicating that said electronic ticket is authentic,
wherein said ticket program includes:
electronic ticket state management information; and
ticket program data for specifying an operation to be performed by said electronic ticket, and
wherein the digital signature of the owner of said service providing means is provided for said presented ticket information.

88. A mobile electronic commerce system according to claim 87, wherein said ticket program includes a ticket signature private key that is employed for a digital signature provided for said electronic ticket, and wherein said ticket certificate is a public key certificate verifying that a ticket signature public key that is paired with said ticket signature private key is authentic.

89. A mobile electronic commerce system according to claim 87, wherein an examination program module for said electronic ticket includes two cryptographic keys, a gate authentication private key and a ticket

authentication public key, and wherein said ticket card program includes a gate authentication public key, which is paired with said gate authentication private key, and a ticket authentication private key, which is paired with said ticket authentication public key.

90. A mobile electronic commerce system according to claim 87, wherein said ticket program data includes:

a transaction module program for specifying the procedures to be used for message data that are exchanged by said electronic wallet and said electronic ticket examination means;
a display module program for specifying the manner in which said electronic ticket is to be displayed; and
representative component information for said electronic ticket, and
wherein a central processing unit in said electronic wallet processes, in accordance with said transaction module program for said electronic ticket, said message data that are exchanged with said electronic ticket examination means, and displays said representative component information in accordance with said display module program for said electronic ticket, so that on display means said electronic ticket is displayed in said electronic wallet.

91. A mobile electronic commerce system according to claim 34, wherein a template program that constitutes a model for said electronic ticket is stored in said ticket issuer information storage means for said service providing means.

92. A mobile electronic commerce system according to claim 91, wherein said template program for said electronic ticket includes:

a transaction module program for said electronic ticket;
a display module program; and
representative component information.

93. A mobile electronic commerce system according to claim 39, wherein identification information that describes a payment method selected by said input means for said electronic wallet is included in said payment card application message issued by said electronic wallet when requesting the purchase of an electronic payment card.

94. A mobile electronic commerce system according to claim 79, wherein said electronic payment card issuance request message or said electronic payment card installation request message includes template program identification information for des-

ignating, in the order to be used for the generation of an electronic payment card, one of a plurality of template programs that are stored in said payment card issuer information storage means.

95. A mobile electronic commerce system according to claim 78, wherein said electronic payment card issuance request message or said electronic payment card installation request message includes representative component information describing the representative component information to be used for an electronic payment card that is to be generated.

96. A mobile electronic commerce system according to claim 76, wherein said electronic wallet generates and then transmits, to said service providing means, a payment card registration request message requesting that said service providing means register, as an electronic payment card that is to be used by the owner of said electronic wallet, said electronic payment card stored in said second storage means for said electronic wallet; wherein said service providing means, upon receiving said payment card registration request message, newly generates, for said electronic payment card, a card signature private key, a card signature public key and a registered card certificate for authenticating said card signature public key, registers said electronic payment card for use in said service director information storage means, and then transmits, to said electronic wallet, said card signature private key and said registered card certificate; and wherein said electronic wallet updates said card signature private key and said registered card certificate that are in storage by replacing them with those that have newly been received, and changes said state management information for said electronic payment card to a usable state.

97. A mobile electronic commerce system according to claim 28, wherein said electronic wallet employs an electronic payment card, which is selected by input means for said electronic wallet from among those stored in said second storage means, to generate a micro-check message that verifies a payment corresponding to an amount entered by said input means, and transmits said micro-check message to said electronic payment card settlement means.

98. A mobile electronic commerce system according to claim 28, wherein said electronic wallet employs an electronic payment card, which is selected by input means of said electronic wallet from among those stored in said second storage means, to generate a payment offer message that offers a payment corresponding to an amount entered by said input means, and transmits said payment offer message

to said electronic payment card settlement means; wherein said electronic payment card settlement means, upon receiving said payment offer message, generates and then transmits, to said electronic wallet, a payment offer response message that assesses a charge corresponding to an amount entered by input means for said electronic payment card settlement means; wherein said electronic wallet, upon receiving said payment offer response message and if said assessed charge is equal to or smaller than an amount entered by said input means for said electronic wallet, subtracts said assessed charge from a remaining amount stored on said electronic payment card, and generates and then transmits, to said electronic payment card settlement means, a micro-check message validating a payment corresponding to said assessed charge; wherein said electronic payment card settlement means stores said received micro-check message in said second storage means for said electronic payment card settlement means, and generates and then transmits, to said electronic wallet, a receipt message confirming that said micro-check message has been received; and wherein said electronic wallet stores said received receipt message in said second storage means for said electronic wallet.

99. A mobile electronic commerce system according to claim 28, wherein said payment offer message includes:

a payment amount entered by said input means of said electronic wallet;
presented card information and a registered card certificate for said electronic payment card; and
state management information to which a digital signature has been added using said card signature private key.

100. A mobile electronic commerce system according to claim 76, wherein said micro-check message includes:

a payment amount;
an amount remaining stored on said electronic payment card;
identification information for said electronic payment card settlement means; and
identification information for the owner of said electronic payment card settlement means. Further, a digital signature is provided for said micro-check message by using said card signature private key for said electronic payment card.

101. A mobile electronic commerce system according to

claim 100, wherein the digital signature of the owner of said electronic wallet is also provided for said micro-check message.

102.A mobile electronic commerce system according to claim 40, wherein said micro-check message includes a micro-check issuing number representing the order in which micro-check messages are generated by said electronic payment card.

103.A mobile electronic commerce system according to claim 98, wherein, at a time designated by said service providing means, said electronic payment card settlement means generates an upload data message that includes data stored in said second storage means for said electronic payment card settlement means, and then transmits said upload data message to said service providing means; wherein said service providing means, upon receiving said upload data message, examines the validity of a micro-check that is included in said upload data message by comparing said micro-check with registration information for said electronic payment card that is registered in said service director information storage means, and generates and then transmits, to said electronic payment card settlement means, an update data message that includes update data for said second storage means for said electronic payment card settlement means; and wherein said electronic payment card settlement means extracts said update data from said update data message that is received, and updates data stored in said second storage means.

104.A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates a payment card transfer offer message containing an offer to transfer, to a second electronic wallet, an electronic payment card that is stored in said second storage means, and then transmits said payment card transfer offer message, via said wireless communication means, to said second electronic wallet; wherein said second electronic wallet, upon receiving said payment card transfer offer message, generates a payment card transfer offer response message indicating that the contents of said payment card transfer offer message are accepted, and then transmits said payment card transfer offer response message, via said wireless communication means, to said first electronic wallet; and wherein said first electronic wallet, upon receiving said payment card transfer offer response message, generates and then transmits, to said second electronic wallet, a payment card transfer certificate message confirming the transfer of said electronic payment card to said second electronic wallet.

105.A mobile electronic commerce system according to claim 104, wherein said payment card transfer offer message includes:

presented card information, and a card certificate or a registered card certificate for said electronic payment card; and state management information having an added digital signature prepared using a card signature private key.

106.A mobile electronic commerce system according to claim 104, wherein said payment card transfer offer message includes a public key certificate for the owner of said first electronic wallet; wherein a digital signature of said owner of said first electronic wallet is provided for said payment card transfer offer message; wherein said payment card transfer offer response message includes a public key certificate for the owner of said second electronic wallet; wherein a digital signature of said owner of said second electronic wallet is provided for said payment card transfer offer message; wherein said payment card transfer certificate message includes identification information for said public key certificate of said owner of said first electronic wallet and identification information for said public key certificate of said owner of said second electronic wallet; and wherein a digital signature using a card signature private key for said electronic payment card and a digital signature of said owner of said first electronic wallet are provided for said payment card transfer certificate message.

107.A mobile electronic commerce system according to claim 42, wherein identification information that describes a payment method selected by said input means of said electronic wallet is included in said telephone card application message issued by said electronic wallet when requesting the purchase of an electronic telephone card.

108.A mobile electronic commerce system according to claim 85, wherein said electronic telephone card issuance request message or said electronic telephone card installation request message includes template program identification information for designating, following the order that is to be used for the generation of electronic telephone cards, one of a plurality of template programs that are stored in said telephone card issuer information storage means.

109.A mobile electronic commerce system according to claim 84, wherein said electronic telephone card issuance request message or said electronic telephone card installation request message includes representative component information describing

representative component information to be used for an electronic telephone card that is to be generated.

110. A mobile electronic commerce system according to claim 82, wherein said electronic wallet generates and then transmits, to said service providing means, a telephone card registration request message requesting that said service providing means register, as an electronic telephone card that is to be used by the owner of said electronic wallet, said electronic telephone card stored in said second storage means for said electronic wallet; wherein said service providing means, upon receiving said telephone card registration request message, newly generates, for said electronic telephone card, a card signature private key, a card signature public key and a registered card certificate for confirming said card signature public key, registers for use said electronic telephone card in said service director information storage means, and then transmits, to said electronic wallet, said card signature private key and said registered card certificate; and wherein said electronic wallet updates said card signature private key and said registered card certificate that are in storage by replacing them with those that have newly been received, and changes said state management information for said electronic telephone card to a usable state.
111. A mobile electronic commerce system according to claim 28, wherein said electronic wallet employs an electronic telephone card, which is selected by input means for said electronic wallet from among those stored in said second storage means, to generate a micro-check message verifying a payment corresponding to an amount entered by said input means, and transmits said micro-check message to said electronic telephone card settlement means.
112. A mobile electronic commerce system according to claim 28, wherein said electronic wallet employs an electronic telephone card, which is selected by input means for said electronic wallet from among those stored in said second storage means, to generate a micro-check call request message requesting a radio communication service in order to communicate with a side that is designated by said input means, and transmits said micro-check call request message to said electronic telephone card settlement means; wherein said electronic telephone card settlement means, upon receiving said micro-check call request message, generates and then transmits, to said electronic wallet, a micro-check call response message for an amount charged that corresponds to a communication fee; said electronic wallet, upon receiving said micro-check call response message, subtracts the

amount charged from the remaining amount stored on said electronic telephone card, and generates and then transmits, to said electronic telephone card settlement means, a telephone micro-check message verifying the payment of an amount corresponding to said amount charged; wherein said electronic telephone card settlement means, upon receiving said telephone micro-check message, generates and then transmits, to said electronic wallet, a receipt message confirming the receipt of said telephone micro-check message; and wherein said electronic wallet stores said received receipt message in said second storage means for said electronic wallet.

113. A mobile electronic commerce system according to claim 28, wherein said electronic telephone card settlement means, when radio wireless communication service is provided, generates and then transmits, to said electronic wallet, a communication fee charge message for an amount charged that corresponds to an additional communication fee; wherein said electronic wallet, upon receiving said communication fee charge message, subtracts said amount that is charged from an amount remaining on said electronic telephone card, and generates and then transmits, to said electronic telephone card settlement means, a new telephone micro-check message verifying payment of the total amount charged; wherein said electronic telephone card settlement means generates and then transmits, to said electronic wallet, a receipt message confirming that said telephone micro-check message has been received; wherein said electronic wallet updates a receipt message stored in said second storage means for said electronic wallet by storing therein said receipt message that is newly received; and wherein said electronic telephone card settlement means, when provision of said radio wireless communication service is terminated, stores the latest telephone micro-check message in said second storage means for said electronic telephone card settlement means.

114. A mobile electronic commerce system according to claim 112 or 113, wherein said micro-check call request message includes:

identification information for said side that is designated by said input means of said electronic wallet;
presented card information and a registered card certificate for said electronic telephone card; and
state management information accompanied by a digital signature that is provided by using a card signature private key.

115.A mobile electronic commerce system according to claim 82, wherein said telephone micro-check message includes:

a payment amount; 5
 a amount remaining stored on said electronic telephone card;
 identification information for said electronic telephone card settlement means; and
 identification information for the owner of said electronic telephone card settlement means, 10
 and
 wherein a digital signature is provided for said telephone micro-check message by using said card signature private key of said electronic telephone card. 15

116.A mobile electronic commerce system according to claim 115, wherein not only said digital signature using said card signature private key for said electronic telephone card, but also the digital signature of the owner of said electronic wallet is provided for said telephone micro-check message. 20

117.A mobile electronic commerce system according to claim 43, wherein said telephone micro-check message includes a telephone micro-check issuing number representing the order in which telephone micro-check messages are generated by said electronic telephone card. 25 30

118.A mobile electronic commerce system according to claim 113, wherein, at a time designated by said service providing means, said electronic telephone card settlement means generates an upload data message that includes data stored in said second storage means for said electronic telephone card settlement means, and then transmits said upload data message to said service providing means; wherein said service providing means, upon receiving said upload data message, examines the validity of a telephone micro-check that is included in said upload data message by comparing said telephone micro-check with registration information for said electronic telephone card that is registered in said service director information storage means, and generates and then transmits, to said electronic telephone card settlement means, an update data message that includes update data for said second storage means for said electronic telephone card settlement means; and wherein said electronic telephone card settlement means extracts said update data from said update data message that is received, and updates data stored in said second storage means. 35 40 45 50 55

119.A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates

a telephone card transfer offer message offering to transfer, to a second electronic wallet, an electronic telephone card that is stored in said second storage means, and transmits said telephone card transfer offer message via said wireless communication means to said second electronic wallet; wherein said second electronic wallet, upon receiving said telephone card transfer offer message, generates a telephone card transfer offer response message indicating that the contents of said telephone card transfer offer message are accepted, and then transmits said telephone card transfer offer response message via said wireless communication means to said first electronic wallet; and wherein said first electronic wallet, upon receiving said telephone card transfer offer response message, generates and then transmits, to said second electronic wallet, a telephone card transfer certificate message confirming the transfer of said electronic telephone card to said second electronic wallet.

120.A mobile electronic commerce system according to claim 119, wherein said telephone card transfer offer message includes:

presented card information and a card certificate or a registered card certificate for said electronic telephone card; and
 state management information accompanied by a digital signature added by using a card signature private key.

121.A mobile electronic commerce system according to claim 119, wherein said telephone card transfer offer message includes a public key certificate for the owner of said first electronic wallet; the digital signature of said owner of said first electronic wallet is provided for said telephone card transfer offer message; wherein said telephone card transfer offer response message includes a public key certificate for the owner of said second electronic wallet; wherein the digital signature of said owner of said second electronic wallet is provided for said telephone card transfer offer message; wherein said telephone card transfer certificate message includes identification information for said public key certificate for said owner of said first electronic wallet and identification information for said public key certificate for said owner of said second electronic wallet; and wherein a digital signature using a card signature private key for said electronic telephone card and the digital signature of said owner of said first electronic wallet are provided for said telephone card transfer certificate message.

122.A mobile electronic commerce system according to claim 45, wherein identification information that

describes a payment method selected by said input means of said electronic wallet is included in said ticket application message issued by said electronic wallet when requesting the purchase of an electronic ticket.

123. A mobile electronic commerce system according to claim 91, wherein said electronic ticket issuance request message or said electronic ticket installation request message includes template program identification information for designating, following the order that is to be used for the generation of electronic tickets, one of a plurality of template programs that are stored in said ticket issuer information storage means.

124. A mobile electronic commerce system according to claim 90, wherein said electronic ticket issuance request message or said electronic ticket installation request message includes representative component information describing representative component information for an electronic ticket that is to be generated.

125. A mobile electronic commerce system according to claim 88, wherein said electronic wallet generates and then transmits, to said service providing means, a ticket registration request message requesting that said service providing means register, as an electronic ticket that is to be used by the owner of said electronic wallet said electronic ticket stored in said second storage means for said electronic wallet; wherein said service providing means, upon receiving said ticket registration request message, newly generates, for said electronic ticket, a ticket signature private key, a ticket signature public key and a registered ticket certificate for verifying said ticket signature public key, registers said electronic ticket for use in said service director information storage means, and then transmits, to said electronic wallet, said ticket signature private key and said registered ticket certificate; and wherein said electronic wallet updates said ticket signature private key and said registered ticket certificate that are stored by replacing them with those that have been newly received, and changes said state management information for said electronic ticket to a usable state.

126. A mobile electronic commerce system according to claim 28, wherein said electronic wallet generates a ticket presenting message in which is designated an electronic ticket that is selected, from among those stored in said second storage means, by input means for said electronic wallet, and transmits said ticket presenting message to said electronic ticket examination means.

127. A mobile electronic commerce system according to claim 126, wherein said electronic ticket examination means, upon receiving said ticket presenting message, generates and then transmits, to said electronic wallet, a ticket examination message instructing the modification of said electronic ticket to a post-examined state; wherein said electronic wallet, upon receiving said ticket examination message, changes said electronic ticket to said post-examined state, and generates and then transmits, to said electronic ticket examination means, a ticket examination response message that describes the contents of the modified electronic ticket; wherein said electronic ticket examination means stores said received ticket examination response message in said second storage means for said electronic ticket examination means, and generates and then transmits, to said electronic wallet, an examination certificate message certifying that said electronic ticket has been examined; and wherein said electronic wallet stores said received examination certificate message in said second storage means for said electronic wallet.

128. A mobile electronic commerce system according to claim 126, wherein said ticket presenting message includes:

presented ticket information and a registered ticket certificate for said electronic ticket; and state management information accompanied by a digital signature provided by using a ticket signature private key.

129. A mobile electronic commerce system according to claim 88, wherein said ticket examination response message includes:

state management information for said electronic ticket; identification information for said electronic ticket examination means; and identification information for the owner of said electronic ticket examination means, and wherein a digital signature is provided for said ticket examination response message by using said ticket signature private key for said electronic ticket.

130. A mobile electronic commerce system according to claim 129, wherein said ticket examination response message includes identification information for said electronic ticket examination means and identification information for the owner of said electronic ticket examination means, and wherein said digital signature prepared using said ticket signature private key for said electronic ticket and the digital signature of the owner of said electronic wal-

let are provided for said ticket examination response message.

131. A mobile electronic commerce system according to claim 47, wherein said ticket examination response message includes a ticket examination number representing the order in which ticket examination response messages are generated by said electronic ticket. 5
132. A mobile electronic commerce system according to claim 127, wherein, at a time designated by said service providing means, said electronic ticket examination means generates an upload data message that includes data stored in said second storage means for said electronic ticket examination means, and then transmits said upload data message to said service providing means; wherein said service providing means, upon receiving said upload data message, determines the validity of a ticket examination response that is included in said upload data message by comparing said ticket examination response with registration information for said electronic ticket that is registered in said service director information storage means, and generates and then transmits, to said electronic ticket examination means, an update data message that includes update data for said second storage means for said electronic ticket examination means; and wherein said electronic ticket examination means extracts said update data from said update data message that is received, and updates data stored in said second storage means. 10 15 20 25 30
133. A mobile electronic commerce system according to claim 28, wherein a first electronic wallet generates a ticket transfer offer message offering to transfer, to a second electronic wallet, an electronic ticket that is stored in said second storage means, and then transmits said ticket transfer offer message via said wireless communication means to said second electronic wallet; wherein said second electronic wallet, upon receiving said ticket transfer offer message, generates a ticket transfer offer response message indicating the contents of said ticket transfer offer message are acceptable, and then transmits said ticket transfer offer response message via said wireless communication means to said first electronic wallet; and wherein said first electronic wallet, upon receiving said ticket transfer offer response message, generates and then transmits, to said second electronic wallet, a ticket transfer certificate message confirming the transfer of said electronic ticket to said second electronic wallet. 35 40 45 50 55
134. A mobile electronic commerce system according to claim 133, wherein said ticket transfer offer message includes:

presented ticket information and a ticket certificate or a registered ticket certificate for said electronic ticket; and

state management information accompanied by a digital signature that is added by using a ticket signature private key.

135. A mobile electronic commerce system according to claim 133, wherein said ticket transfer offer message includes a public key certificate for the owner of said first electronic wallet; wherein the digital signature of said owner of said first electronic wallet is provided for said ticket transfer offer message; wherein said ticket transfer offer response message includes a public key certificate for the owner of said second electronic wallet; wherein the digital signature of said owner of said second electronic wallet is provided for said ticket transfer offer message; wherein said ticket transfer certificate message includes identification information for said public key certificate for said owner of said first electronic wallet and identification information for said public key certificate for said owner of said second electronic wallet; and wherein a digital signature using a ticket signature private key for said electronic ticket and the digital signature of said owner of said first electronic wallet are provided for said ticket transfer certificate message.
136. A mobile electronic commerce system according to claim 39, wherein settlement option information for deciding which procedures to use for settlement is included in said electronic payment card issuance request message, in said electronic telephone card issuance request message or in said electronic ticket issuance request message.
137. A mobile electronic commerce system according to claim 136, wherein said service providing means, upon receiving said electronic payment card issuance request message, said electronic telephone card issuance request message or said electronic ticket issuance request message, generates and then transmits, to said electronic wallet, an electronic payment card, an electronic telephone card or an electronic ticket before performing a price settlement in accordance with said settlement option information.
138. A mobile electronic commerce system according to claim 39, wherein said service providing means, upon receiving said electronic payment card issuance request message, said electronic telephone card issuance request message or said electronic ticket issuance request message, generates and then transmits, to said electronic wallet, an electronic payment card, an electronic telephone card or an electronic ticket, and a temporary receipt

message describing the contents of a settlement before performing a price settlement in accordance with said settlement option information.

139. A mobile electronic commerce system according to claim 28, wherein data concerning said electronic payment card, said electronic telephone card and said electronic ticket belonging to the owner of said electronic wallet, and data processed by said central processing unit of said electronic wallet are stored in said second storage means for said electronic wallet or in said user information storage means for said service providing means; wherein said data are managed by describing, in said second storage means for said electronic wallet, identification information for said data, and addresses of said data in said corresponding storage means; wherein, when data at an address in said user information storage means are to be processed, said electronic wallet generates and then transmits, to said service providing means, a remote access request message requesting address data; wherein said service providing means, upon receiving said remote access request message, generates and then transmits, to said electronic wallet, a remote access data message in which said requested data are included; and wherein said electronic wallet, upon receiving said remote access data message, extracts said requested data from said message.
140. A mobile electronic commerce system according to claim 1, wherein said electronic wallet employs a ferroelectric nonvolatile memory as storage means.
141. A mobile electronic commerce system according to claim 10, wherein a ferroelectric nonvolatile memory is employed as storage means for said electronic payment card settlement means.
142. A printed matter according to claim 63, wherein said object is one whereon or wherein electronic payment card installation information, electronic telephone card installation information, or electronic ticket installation information is printed or engraved in a form readable by a person or reading means.
143. A printed matter according to claim 142, wherein a coating is applied to a portion of said object whereon or wherein said electronic payment card installation information, said electronic telephone card installation information or said electronic ticket installation information is printed or engraved in order to disable the reading of said electronic payment card installation information, said electronic telephone card installation information or said electronic ticket installation information, and wherein said coating is removable.
144. A printed matter according to claim 142, wherein, to prevent holographic counterfeiting, a micro-character or a micro-pattern is printed on or etched in said object.
145. A recording medium according to claim 64, on which electronic payment card installation information, electronic telephone card installation information, or electronic ticket installation information is recorded using a form that is readable by recording/reproduction means.
146. A recording medium, on which a control program for said central processing unit of said electronic wallet defined in claim 28 is stored in a form readable by a computer.
147. A recording medium, on which a control program for said central processing unit of said electronic payment card settlement means defined in claim 29 is recorded in a form readable by a computer.
148. A recording medium, on which a control program for said central processing unit of said electronic telephone card settlement means defined in claim 32 is recorded in a form readable by a computer.
149. A recording medium, on which a control program for said central processing unit of said electronic ticket examination means defined in claim 33 is recorded in a form readable by a computer.
150. A recording medium, on which a processing program for said computer system of said service providing means defined in claim 34 is recorded in a form readable by a computer.
151. A recording medium, on which a processing program for said computer system of said settlement processing means defined in claim 35 is recorded in a form readable by a computer.
152. A recording medium, on which a processing program for said computer system of said payment card issuing means defined in claim 36 is recorded in a form readable by a computer.
153. A recording medium, on which a processing program for said computer system of said telephone card issuing means defined in claim 37 is recorded in a form readable by a computer.
154. A recording medium, on which a processing program for said computer system of said ticket issuing means defined in claim 38 is recorded in a form readable by a computer.
155. An electronic wallet used for a mobile electronic

commerce system for paying, via wireless communication means, a required amount from said electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, said electronic wallet comprising:

input means for entering a numerical value and for performing a selection operation;
 a central processing unit for generating data to be transmitted via said wireless communication means, and for processing data received via said wireless communication means;
 first storage means for storing a control program for controlling an operation performed by said central processing unit;
 display means for displaying data processed by said central processing unit;
 second storage means for storing said data processed by said central processing unit, and an electronic negotiable card received through said wireless communication means; and
 third storage means for storing identification information and authorization information for the user of said electronic wallet,
 wherein for carrying, said third storage means is detachable from said electronic wallet,
 wherein, when said third storage means is removed from said electronic wallet, said electronic negotiable card stored in said second storage means is erased, and
 wherein, when said third storage means is attached to said electronic wallet, said electronic wallet communicates with said service providing means via said wireless communication means, and receives said electronic negotiable card that said user of said electronic wallet owns and stores said electronic negotiable card in said second storage means.

156.An electronic wallet, used for a mobile electronic commerce system for paying, via wireless communication means, a required amount from said electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, said electronic wallet comprising:

input means for entering a numerical value and for performing a selection operation;
 a central processing unit for generating data to be transmitted via said wireless communication means, and for processing data received via said wireless communication means;
 first storage means for storing a control program for controlling an operation performed by said central processing unit;
 display means for displaying data processed by

said central processing unit;
 second storage means for storing said data processed by said central processing unit; and
 third storage means for storing an electronic negotiable card received via said wireless communication means,
 wherein for carrying, said third storage means is detachable from said electronic wallet.

157.An electronic wallet, used for a mobile electronic commerce system for paying, via wireless communication means, a required amount from said electronic wallet that includes said wireless communication means and for receiving a product or a service, or a required permission, from a supply side, said electronic wallet comprising:

input means for entering a numerical value and for performing a selection operation;
 a central processing unit for generating data to be transmitted via said wireless communication means, and for processing data received via said wireless communication means;
 first storage means for storing a control program for controlling an operation performed by said central processing unit;
 display means for displaying data processed by said central processing unit;
 second storage means for storing said data processed by said central processing unit; and
 IC card reading/writing means,
 wherein said electronic negotiable card received via said wireless communication means is stored in an IC card that is loaded in said IC card reading/writing means.

158.An electronic wallet comprising:

wireless communication means;
 means for installing a program for an electronic negotiable card obtained from a predetermined agency via said wireless communication means; and
 means for, in order to receive a product or a service from a seller or to obtain a permission, employing said electronic negotiable card with said wireless means in accordance with said program for said electronic negotiable card.

159.An electronic wallet according to claim 158, wherein an inherent private key for providing a digital signature for data to be transmitted to said seller is included in said program for said electronic negotiable card, so that said electronic negotiable card is employed by means provided for employing said electronic negotiable card.

160.An electronic wallet according to claim 158, further

comprising:

means for, when said installation means receives a modification instruction message from said predetermined agency instructing a change to said program for said electronic negotiable card, changing, in accordance with said modification instruction message, said program for said negotiable card that is installed.

161.An electronic wallet according to claim 158, further comprising:

means for, when a modification notification message for the changing of the contents of said program for said electronic negotiable card is received from said predetermined agency, generating a reaction selection message indicating that the modification of the contents of said program is accepted; and means for, when said installation means receives a modification instruction message from said predetermined agency instructing the changing of said program for said electronic negotiable card, changing in accordance with said modification instruction message said program for said negotiable card that is installed.

162.An electronic wallet according to claim 158, further comprising:

means for, when a modification notification message that the contents of said electronic negotiable card is to be changed is received from said predetermined agency, generating a reaction selection message requesting a refund process for said electronic negotiable card, and for transmitting said reaction selection message to said predetermined agency; and means for, when a refund receipt message is received from said predetermined agency indicating the termination of said refund process, deleting said program for said negotiable card that is installed.

163.An electronic wallet according to claim 158, wherein said program for said negotiable card is a coupon ticket that has at least two functions for a payment card, a telephone card and a ticket.

164.A seller terminal comprising:

wireless communication means; means for installing, from a predetermined agency, a program module that defines a settlement process performed by a seller when an

electronic negotiable card is used; and means for, in accordance with said program module, communicating with an electronic wallet via said wireless communication means and for performing said settlement process for said seller when said electronic negotiable card is employed.

165.An automatic vending machine comprising:

wireless communication means; means for installing, from a predetermined agency, a program module that defines a settlement process performed by said automatic vending machine when an electronic negotiable card is used; means for, in accordance with said program module, communicating with an electronic wallet via said wireless communication means and for performing said settlement process for said automatic vending machine when said electronic negotiable card is employed; and means for providing a product or a service when said settlement process for said automatic vending machine has been completed.

166.A call switching center machine comprising:

wireless communication means; means for installing, from a predetermined agency, a program module that defines a settlement process performed by said call switching center machine when an electronic negotiable card is used; means for, in accordance with said program module, communicating with an electronic wallet via said wireless communication means and for performing said settlement process for said call switching center machine when said electronic negotiable card is employed; and means for providing a product or a service when said settlement process for said call switching center machine has been completed.

167.A management machine for a service providing agency comprising:

communication means; means for generating a program for an electronic negotiable card in order to install said program in an electronic wallet, and for transmitting said program for said electronic negotiable card to said electronic wallet by radio via said communication means; and means for transmitting to a seller terminal, in order to install said program in said seller terminal, a program module that defines a settlement process performed by a seller when said

program for said electronic negotiable card is employed.

168.A management machine for a service providing agency comprising:

communication means;

means for receiving from an electronic wallet, by radio via said communication means, a purchase order request for a program for an electronic negotiable card;

means for receiving data, concerning a negotiable card that is to be issued, from a negotiable card issuing agency that issues said electronic negotiable card that is ordered by said purchase order request;

means for performing, together with a settlement agency, a settlement process that accompanies the purchase of said negotiable card;

means for generating a program for an electronic negotiable card, based on data that are received from said negotiable card issuing agency and that concern a negotiable card to be issued, and for transmitting said program for said negotiable card to said electronic wallet by radio via said communication means; and

means for transmitting to a seller terminal, in order to install said program in said seller terminal, a program module that defines a settlement process performed by a seller when said program for said electronic negotiable card is employed.

169.A management machine for a negotiable card program issuing agency according to claim 168, further comprising:

means for generating a modification instruction message for changing said program for said negotiable card that is installed in said electronic wallet; and

means for transmitting said modification instruction message to said electronic wallet via said communication means.

170.A management machine for a negotiable card program issuing agency according to claim 168, further comprising:

means for generating a modification notification message for the modification of said program for said negotiable card that is installed in said electronic wallet;

means for receiving, from said electronic wallet, a reaction selection message indicating said modification has been accepted;

means for, upon receiving said reaction selection message, generating a modification

instruction message for changing said program for said negotiable card that is installed in said electronic wallet; and

means for transmitting said modification instruction message to said electronic wallet via said communication means.

171.A management machine for a negotiable card program issuing agency according to claim 168, further comprising:

means for generating a modification notification message for the modification of said program for said negotiable card that is installed in said electronic wallet;

means for receiving from said electronic wallet, in response to said modification notification, a reaction selection message requesting a refund for said electronic negotiable card;

means for, upon receiving said reaction selection message, performing a refund settlement process for a predetermined settlement agency;

means for generating a refund receipt message indicating that said refund settlement process has been completed; and

means for transmitting said refund receipt message to said electronic wallet via said communication means.

172.A management machine for a service providing agency, which transmits, to an electronic wallet, an electronic negotiable card program, including a card signature private key, a card certificate, a card authorization private key and an accounting machine authorization private key, and which transmits to a seller terminal a settlement program, including a card authorization public key that is paired with said card authorization private key and an accounting machine authorization private key that is paired with said accounting machine authorization public key, said management machine comprising:

means for managing, for each negotiable card type, the pair comprising said card authorization private key, which differs for each negotiable card type, and said card authorization public key, and the pair comprising said accounting machine authorization private key and said accounting machine authorization public key; and

means for, in order to issue a negotiable card, generating a card signature private key, which is inherent to said negotiable card, and a card certificate, and for generating a negotiable card by using said card authorization private key, which corresponds to the type of said negotia-

ble card, and said accounting machine authorization public key.

173.A mobile electronic commerce system according to claim 3, wherein said electronic wallet includes means for generating first identification information for identifying a transaction conducted with said supply side, and for transmitting said first identification information to said supply side; wherein said supply side includes means for generating second identification information for identifying a transaction conducted with said electronic wallet, and for transmitting said second identification information to said electronic wallet; wherein said electronic wallet includes means for generating said electronic check that contains first said information and said second information; and wherein said supply side includes means for generating a receipt that contains said first identification information and said second identification information.

174.A mobile electronic commerce system according to claim 50, wherein said first electronic wallet includes means for generating first identification information for identifying an electronic payment card transfer process performed with said second electronic wallet, and for transmitting said first identification information to said second electronic wallet; wherein said second electronic wallet includes means for generating second identification information for identifying an electronic payment card transfer process performed with said first electronic wallet, and for transmitting said second identification information to said first electronic wallet; wherein said first electronic wallet includes means for generating said payment card transfer certificate message that contains said first identification information and said second identification information; and wherein said second electronic wallet includes means for generating said payment card receipt message that contains said first identification information and said second identification information.

175.A mobile electronic commerce system according to claim 52, wherein said first electronic wallet includes means for generating first identification information for identifying an electronic telephone card transfer process performed with said second electronic wallet, and for transmitting said first identification information to said second electronic wallet; wherein said second electronic wallet includes means for generating second identification information for identifying an electronic telephone card transfer process performed with said first electronic wallet, and for transmitting said second identification information to said first electronic wallet; wherein said first electronic wallet includes means for generating said telephone card transfer certi-

cate message that contains said first identification information and said second identification information; and wherein said second electronic wallet includes means for generating said telephone card receipt message that contains said first identification information and said second identification information.

176.A mobile electronic commerce system according to claim 54, wherein said first electronic wallet includes means for generating first identification information for identifying an electronic ticket transfer process performed with said second electronic wallet, and for transmitting said first identification information to said second electronic wallet; wherein said second electronic wallet includes means for generating second identification information for identifying an electronic ticket transfer process performed with said first electronic wallet, and for transmitting said second identification information to said first electronic wallet; wherein said first electronic wallet includes means for generating said ticket transfer certificate message that contains said first identification information and said second identification information; and wherein said second electronic wallet includes means for generating said ticket receipt message that contains said first identification information and said second identification information.

177.A mobile electronic commerce system according to claim 54, wherein said first electronic wallet includes means for generating first identification information for identifying a negotiable card transfer process performed with said second electronic wallet, and for transmitting said first identification information to said second electronic wallet; wherein said second electronic wallet includes means for generating second identification information for identifying a negotiable card transfer process performed with said first electronic wallet, and for transmitting said second identification information to said first electronic wallet; wherein said first electronic wallet includes means for generating said payment card transfer certificate message that contains said first identification information and said second identification information; and wherein said second electronic wallet includes means for generating said payment card receipt message that contains said first identification information and said second identification information.

178.A recording medium on which is stored a program for an electronic payment card used by an electronic wallet in a mobile electronic commerce system for paying, via wireless communication means, a required amount from said electronic wallet that includes said wireless communication means, and

for receiving a product or a service, or a required permission, from a supply side, and on which said program for said electronic payment card is so stored as to be readable by a computer, wherein said electronic payment card includes a payment card program, presented card information that describes the contents of said electronic payment card that is issued, and a card certificate for proving that said electronic payment card is real; wherein said payment card program further includes management information for the status of said electronic payment card, and payment card program data that specifies the operations performed by said electronic payment card; and wherein said presented card information is accompanied by the digital signature of the owner of the service providing means.

179.A recording medium according to claim 178, wherein said payment card program includes a card signature private key that is used for a digital signature for an electronic payment card, and wherein said card certificate is a public key certificate that verifies a card signature public key that is paired with said card signature private key.

180.A recording medium according to claim 178, wherein a clearing program module for said electronic payment card includes two cryptographic keys, an accounting machine authorization private key and a card authorization public key; and wherein said payment card program includes an accounting machine authorization public key that is paired with said accounting machine authorization private key, and a card authorization private key that is paired with said card authorization public key.

181.A recording medium according to claim 178, whereof said payment card program data includes a transaction module program, for specifying the procedures employed for message data that are exchanged by said electronic wallet and electronic payment card settlement means, a display module program, for specifying a display for an electronic payment card, and representative component information for an electronic payment card; and whereof, in accordance with said transaction module program for said electronic payment card, a central processing unit in said electronic wallet processes said message data that are exchanged with said electronic payment card clearing means, and displays said representative component information in accordance with said display module program for said electronic payment card, so that said electronic payment card is displayed on display means of said electronic wallet.

182.A recording medium on which is stored a program for a negotiable card used by an electronic wallet in a mobile electronic commerce system for paying, via wireless communication means, a required amount from said electronic wallet that includes said wireless communication means, and for receiving a product or a service, or a required permission, from a supply side, and on which said program for said negotiable card is so stored as to be readable by a computer, wherein said negotiable card includes a negotiable card program, presented card information that describes the contents of said negotiable card that is issued, and a card certificate for proving that said negotiable card is authentic; wherein said negotiable card program further includes management information for the status of said negotiable card, and negotiable card program data that specifies the operations performed by said negotiable card; and wherein said presented card information is accompanied by the digital signature of the owner of the service providing means.

183.A recording medium according to claim 182, wherein said electronic negotiable card program includes a card signature private key that is used for a digital signature for an electronic negotiable card, and wherein said card certificate is a public key certificate that verifies a card signature public key that is paired with said card signature private key.

184.A recording medium according to claim 182, wherein a clearing program module for said electronic negotiable card includes two cryptographic keys, an accounting machine authorization private key and a card authorization public key; and wherein said negotiable card program includes an accounting machine authorization public key that is paired with said accounting machine authorization private key, and a card authorization private key that is paired with said card authorization public key.

185.A recording medium according to claim 178, whereof said negotiable card program data includes a transaction module program, for specifying the procedures employed for message data that are exchanged by said electronic wallet and electronic negotiable card settlement means, a display module program, for specifying a display for an electronic negotiable card, and representative component information for an electronic negotiable card; and whereof, in accordance with said transaction module program for said electronic negotiable card, a central processing unit in said electronic wallet processes said message data that are exchanged with said electronic negotiable card clearing means, and displays said representative component information in accordance with said dis-

play module program for said electronic negotiable card, so that said electronic negotiable card is displayed on display means of said electronic wallet.

186. A recording medium on which is stored a program 5
for an electronic telephone card used by an elec-
tronic wallet in a mobile electronic commerce sys-
tem for paying, via wireless communication means,
a required amount from said electronic wallet that 10
includes said wireless communication means, and
for receiving a product or a service, or a required
permission, from a supply side, and on which said
program for said electronic telephone card is so
stored as to be readable by a computer, wherein 15
said electronic telephone card includes a telephone
card program, presented card information that
describes the contents of said electronic telephone
card that is issued, and a card certificate for proving
that said electronic telephone card is authentic; 20
wherein said telephone card program further
includes management information for the status of
said electronic telephone card, and telephone card
program data that specifies the operations per-
formed by said electronic telephone card; and 25
wherein said presented card information is accom-
panied by the digital signature of the owner of the
service providing means.

187. A recording medium on which is stored a program 30
for an electronic telephone card used by an elec-
tronic wallet in a mobile electronic commerce sys-
tem for paying, via wireless communication means,
a required amount from said electronic wallet that
includes said wireless communication means, and 35
for receiving a product or a service, or a required
permission, from a supply side, and on which said
program for said electronic telephone card is so
stored as to be readable by a computer, wherein
said telephone card program includes a card signa- 40
ture private key that is used for a digital signature
for an electronic telephone card, and wherein said
card certificate is a public key certificate that veri-
fies a card signature public key that is paired with
said card signature private key. 45

188. A recording medium on which is stored a program
for an electronic telephone card used by an elec-
tronic wallet in a mobile electronic commerce sys-
tem for paying, via wireless communication means,
a required amount from said electronic wallet that 50
includes said wireless communication means, and
for receiving a product or a service, or a required
permission, from a supply side, and on which said
program for said electronic telephone card is so
stored as to be readable by a computer, whereof, in 55
accordance with said transaction module program
for said electronic telephone card, a central
processing unit in said electronic wallet processes

said message data that are exchanged with said
electronic telephone card clearing means, and dis-
plays said representative component information in
accordance with said display module program for
said electronic telephone card, so that said elec-
tronic telephone card is displayed on display means
of said electronic wallet, and whereof said tele-
phone card program data includes a transaction
module program, for specifying the procedures
employed for message data that are exchanged by
said electronic wallet and electronic telephone card
settlement means, a display module program, for
specifying a display for an electronic telephone
card, and representative component information for
an electronic telephone card.

189. A recording medium on which is stored a program
for an electronic ticket used by an electronic wallet
in a mobile electronic commerce system for paying,
via wireless communication means, a required
amount from said electronic wallet that includes
said wireless communication means, and for
receiving a product or a service, or a required per-
mission, from a supply side, and on which said pro-
gram for said electronic ticket is so stored as to be
readable by a computer, wherein said electronic
ticket includes a ticket program, presented card
information that describes the contents of said elec-
tronic ticket that is issued, and a card certificate for
proving that said electronic ticket is authentic;
wherein said ticket program further includes man-
agement information for the status of said elec-
tronic ticket, and ticket program data that specifies
the operations performed by said electronic ticket;
and wherein said presented card information is
accompanied by the digital signature of the owner
of the service providing means.

190. A recording medium according to claim 189,
wherein said ticket program includes a ticket signa-
ture private key that is used for a digital signature
for an electronic ticket, and wherein said ticket cer-
tificate is a public key certificate that verifies a ticket
signature public key that is paired with said ticket
signature private key.

191. A recording medium according to claim 189,
wherein an examination program module for said
electronic ticket includes two cryptographic keys, a
gate authorization private key and a ticket authori-
zation public key; and wherein said ticket program
includes a gate authorization public key that is
paired with said gate authorization private key, and
a ticket authorization private key that is paired with
said ticket authorization public key.

192. A recording medium according to claim 189,
whereof said ticket program data includes a trans-

action module program, for specifying the procedures employed for message data that are exchanged by said electronic wallet and electronic ticket examination means, a display module program, for specifying a display for an electronic payment card, and representative component information for an electronic ticket; and whereof, in accordance with said transaction module program for said electronic ticket, a central processing unit in said electronic wallet processes said message data that are exchanged with said electronic ticket examination means, and displays said representative component information in accordance with said display module program for said electronic ticket, so that said electronic ticket is displayed on display means of said electronic wallet.

193.A recording medium on which a program for a payment card, which is used for electronic commerce that employs an electronic wallet, is so stored as to be readable by a computer, and whereon as information indicating the contents of a negotiable card, included for said payment card, is ASCII information for which tag information that describes the information type is additionally provided.

194.A recording medium on which a program for a telephone card, which is used for electronic commerce that employs an electronic wallet, is so stored as to be readable by a computer, and whereon as information indicating the contents of an electronic telephone card, included for said telephone card, is ASCII information for which tag information that describes the information type is additionally provided.

195.A recording medium on which a program for a ticket, which is used for electronic commerce that employs an electronic wallet, is so stored as to be readable by a computer, and whereon as information indicating the contents of an electronic ticket, included for said ticket, is ASCII information for which tag information that describes the information type is additionally provided.

FIG. 1

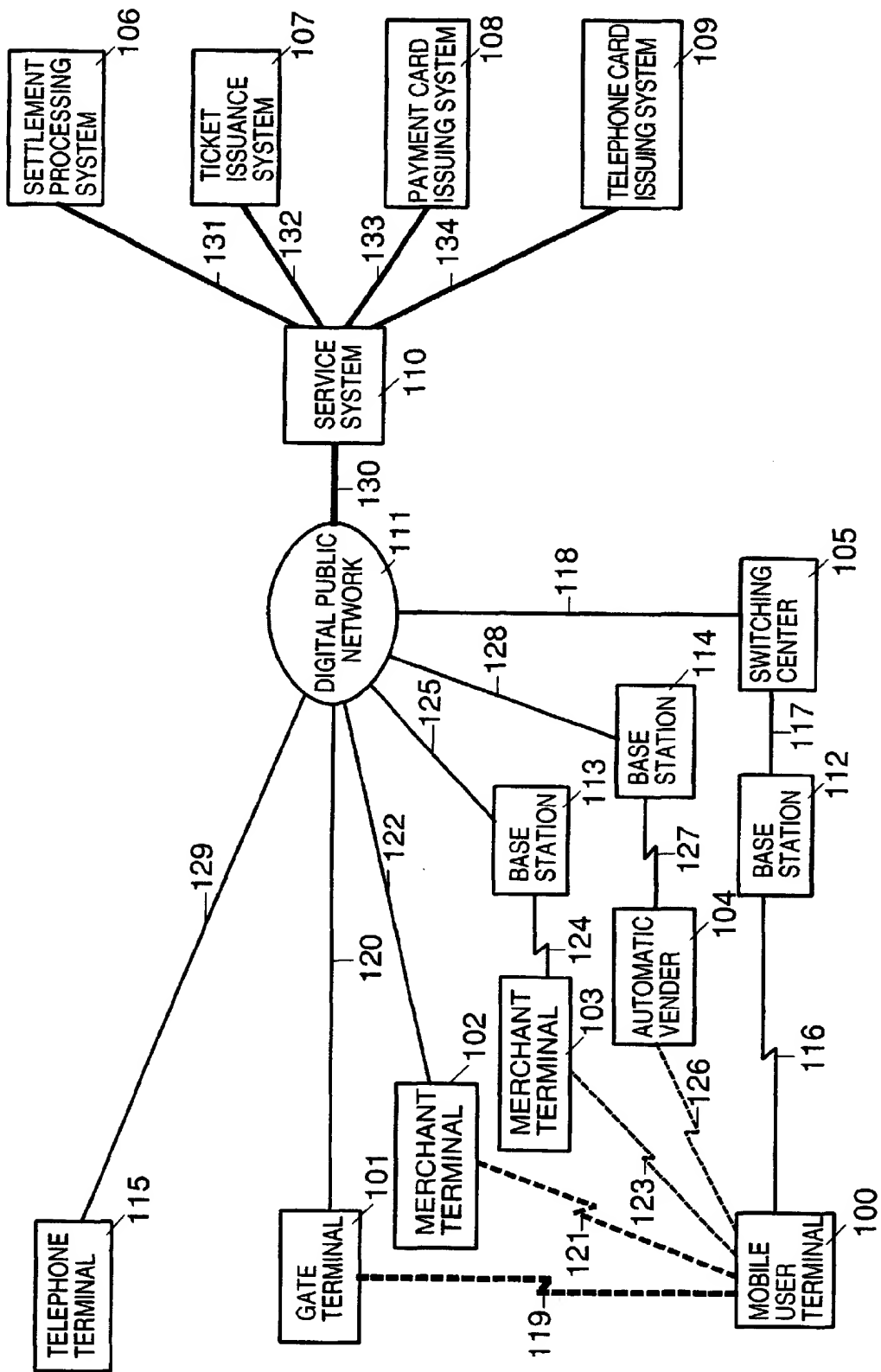


FIG. 2A

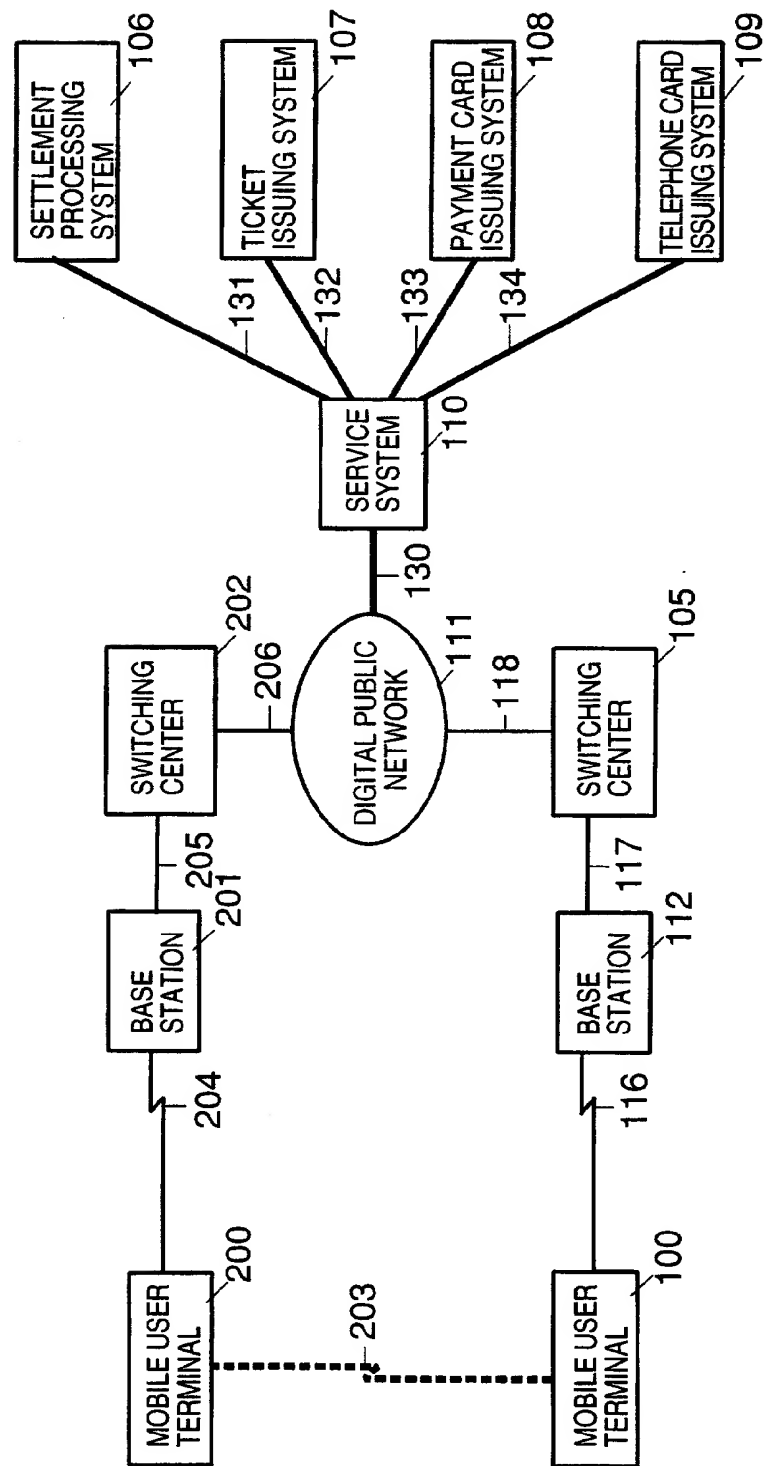


FIG. 2B

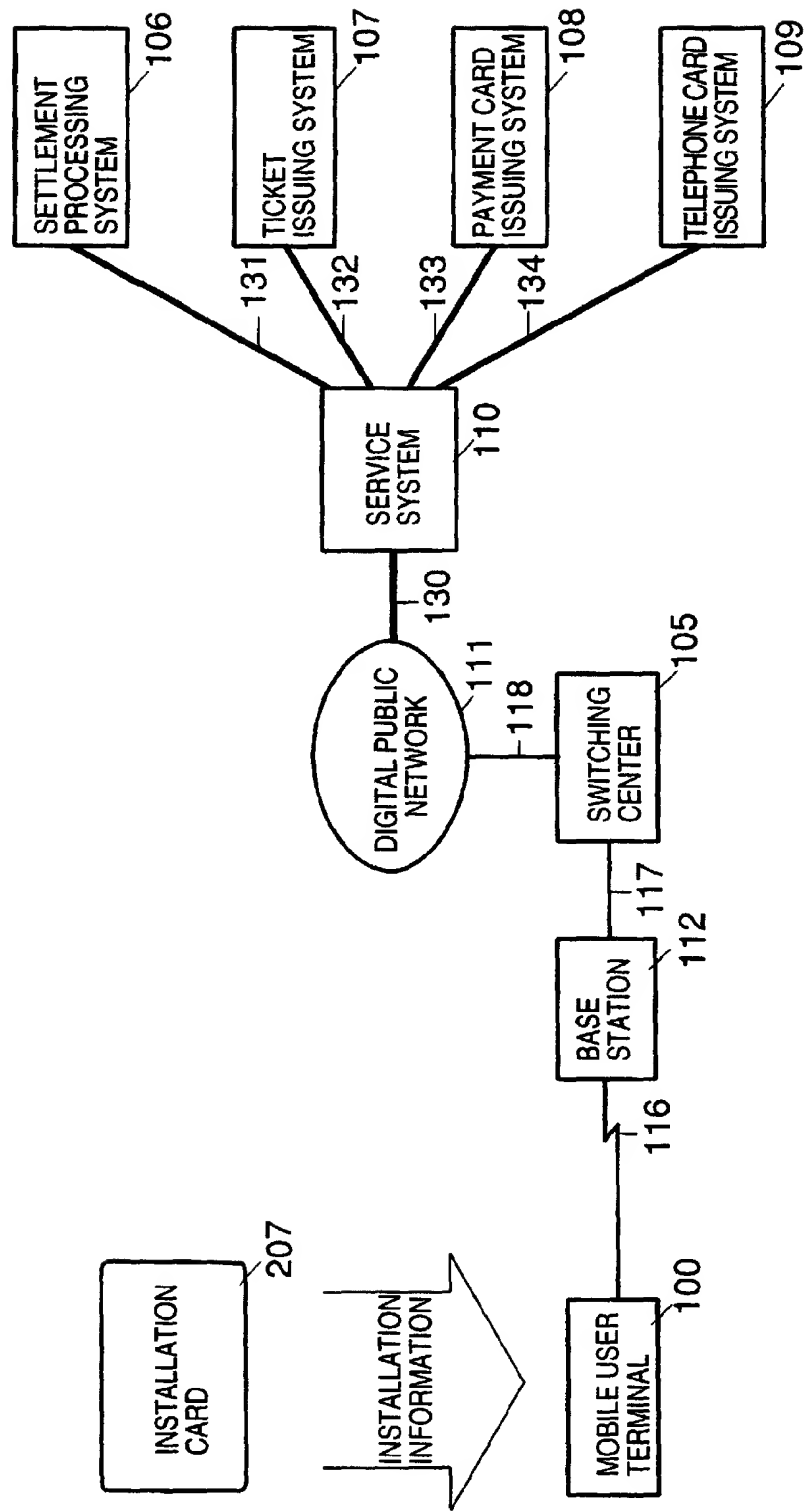


FIG. 3A

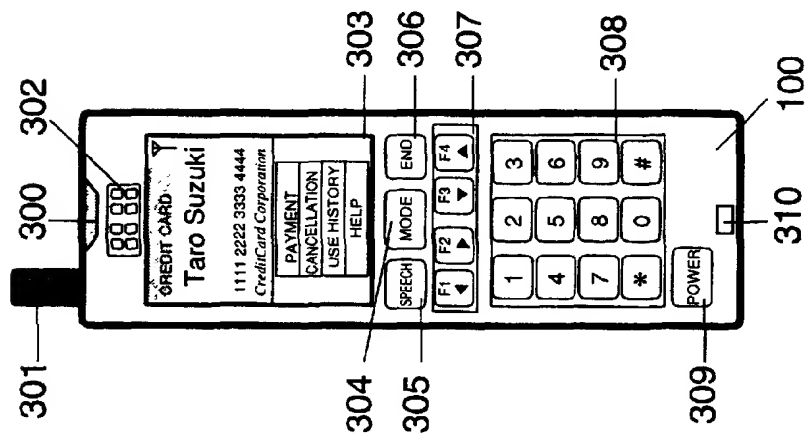


FIG. 3B

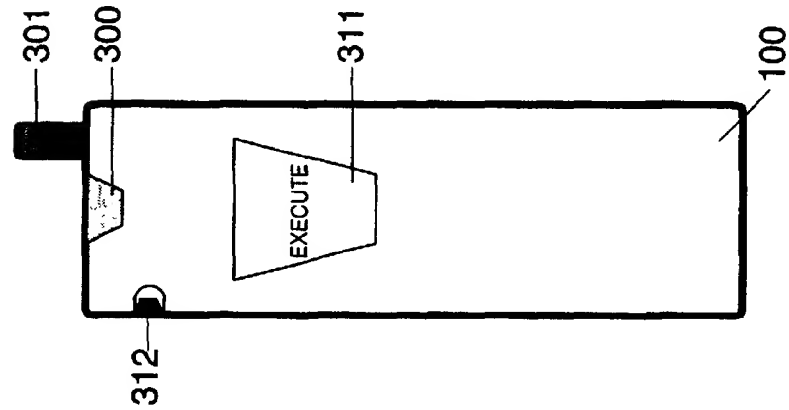


FIG. 3C

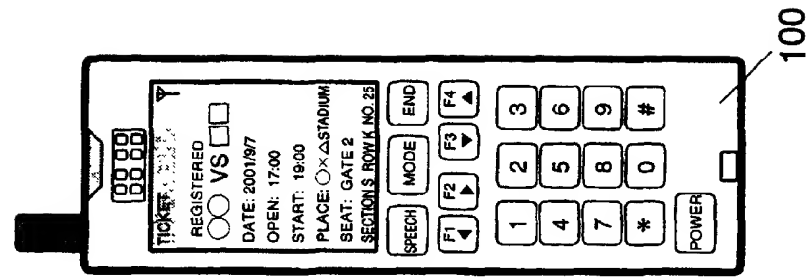


FIG. 3D

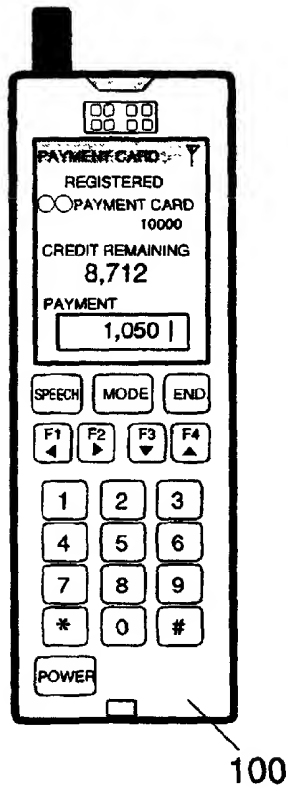


FIG. 3E

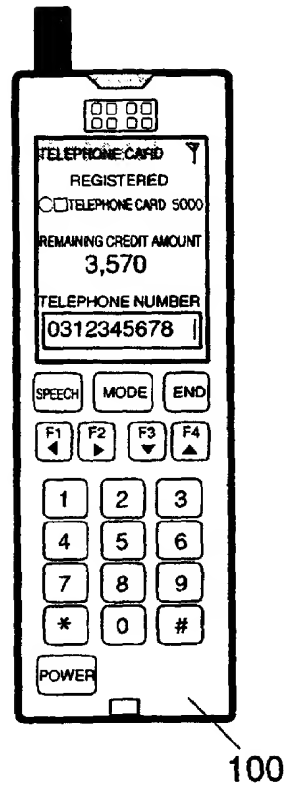


FIG. 3F

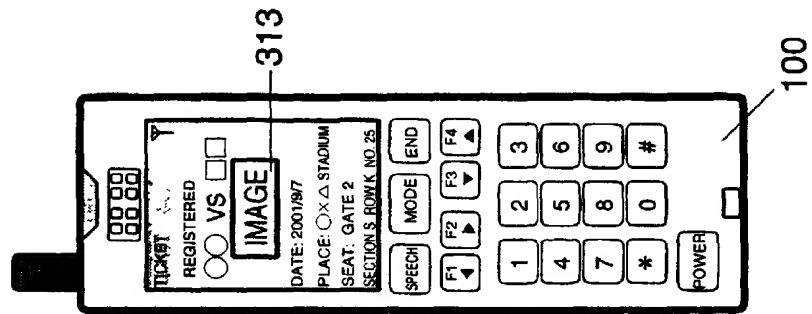


FIG. 3G

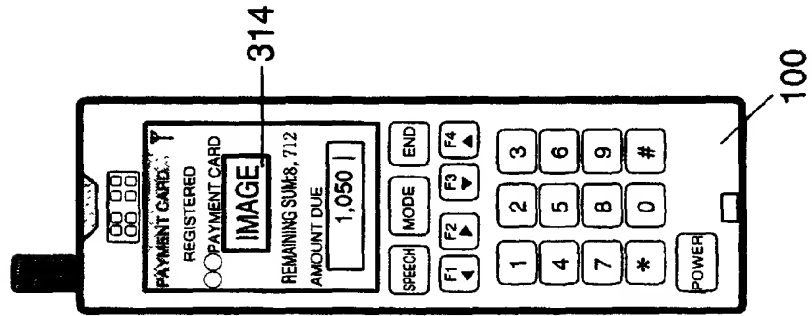


FIG. 3H

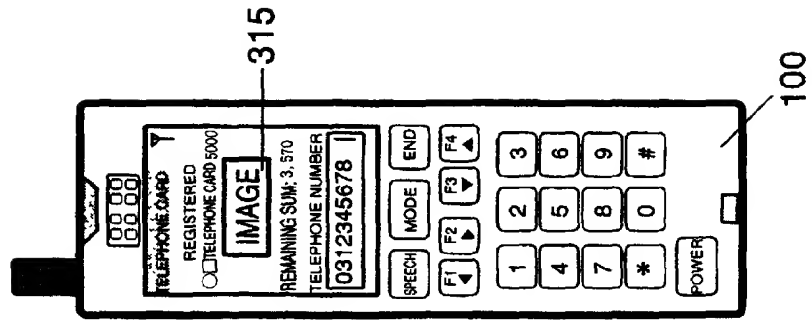


FIG. 4

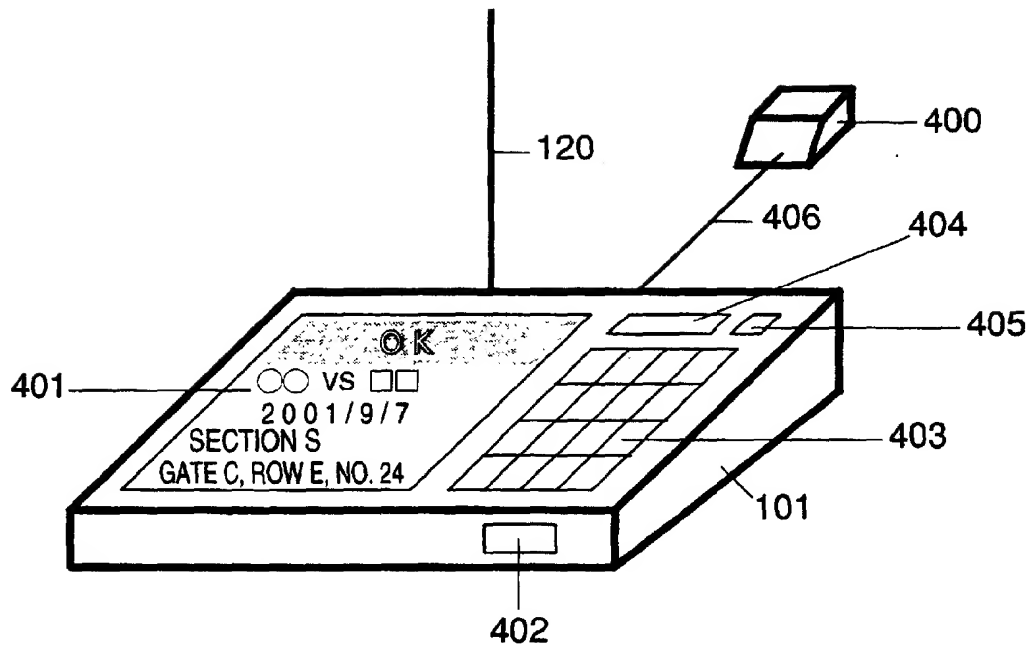


FIG. 5

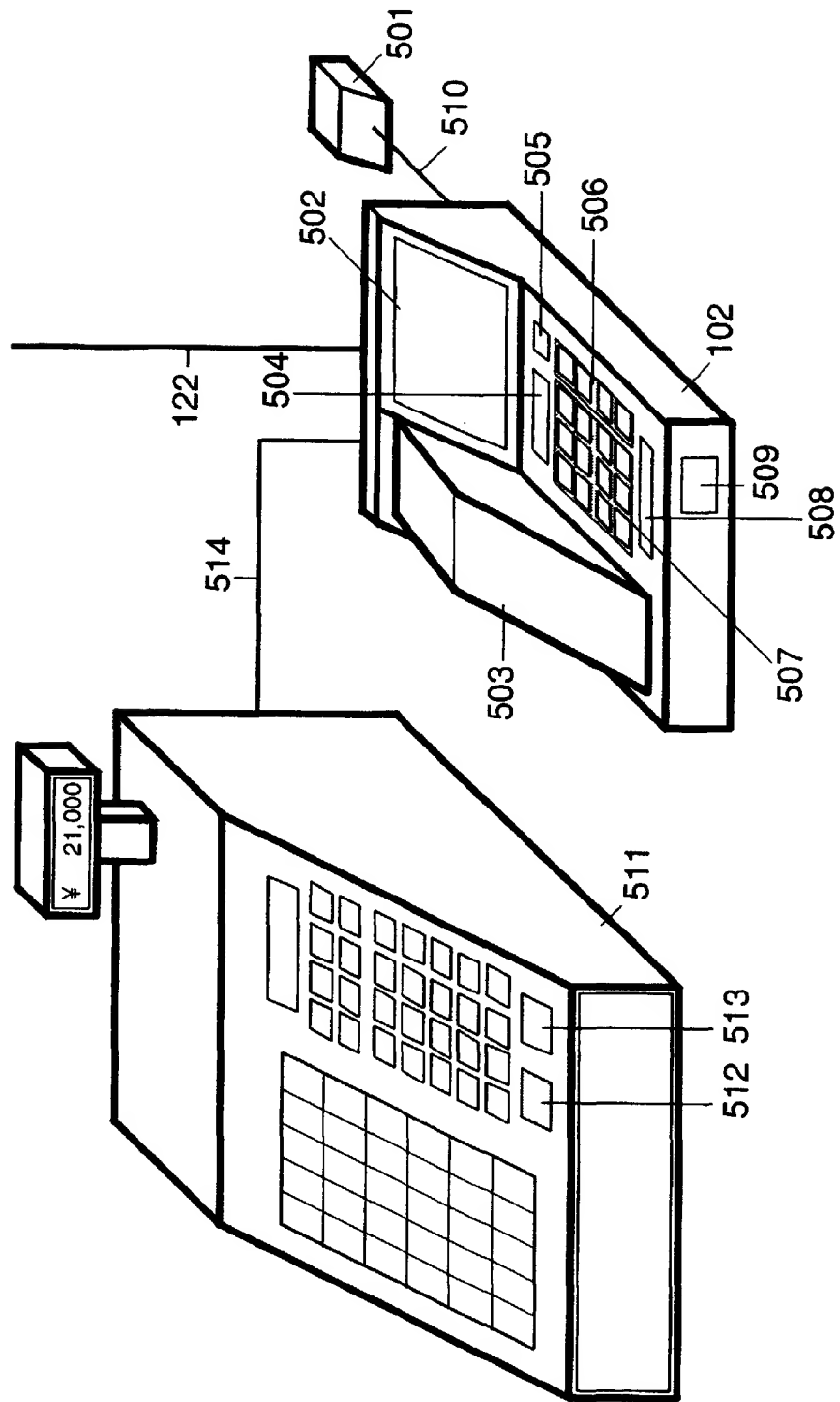


FIG. 6A

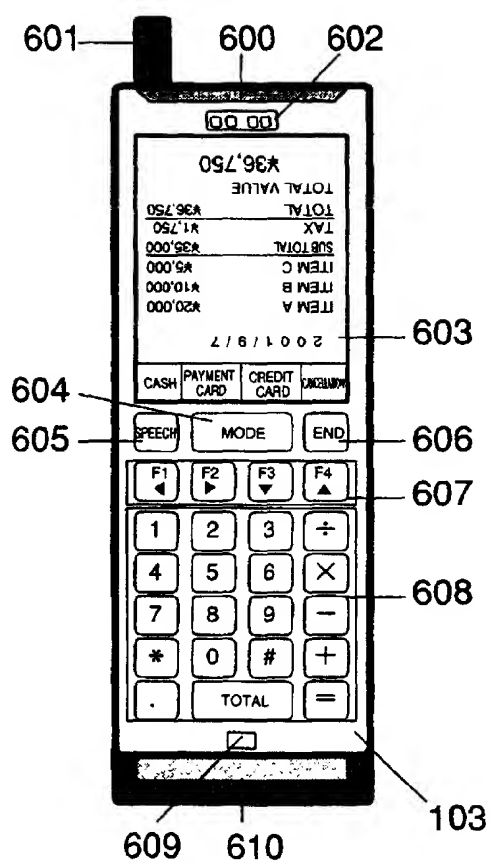


FIG. 6B

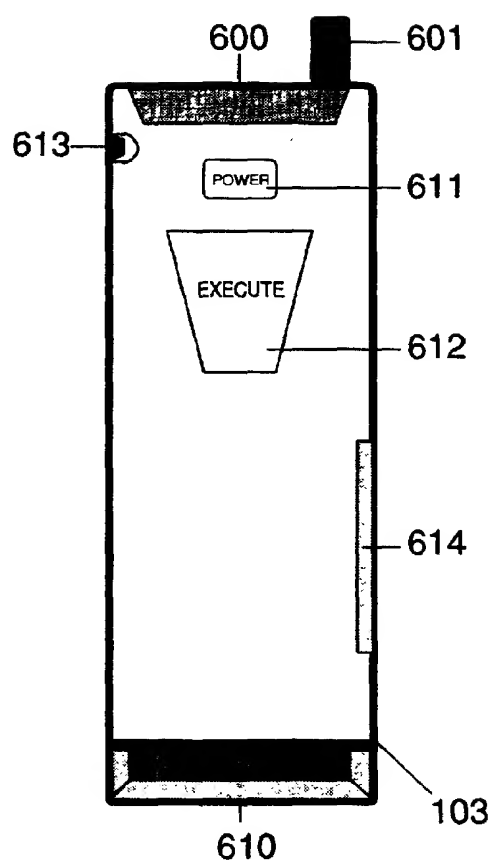


FIG. 7

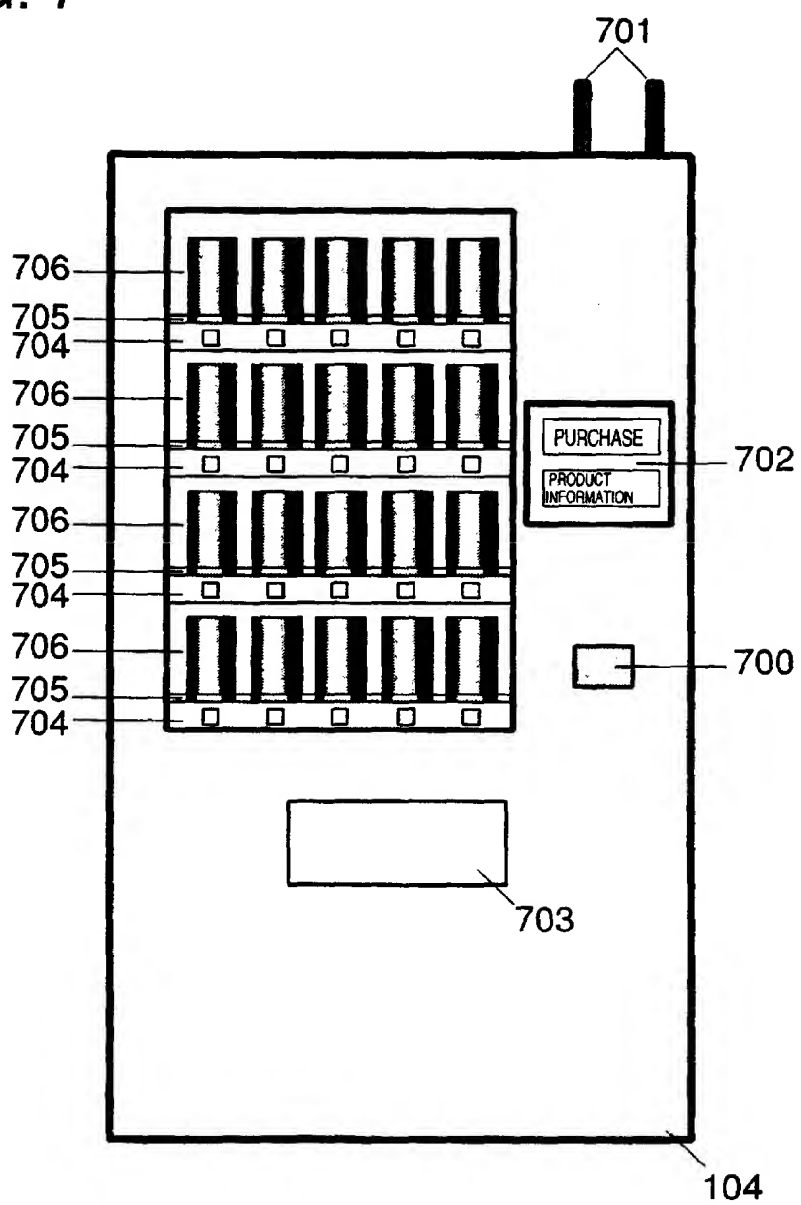
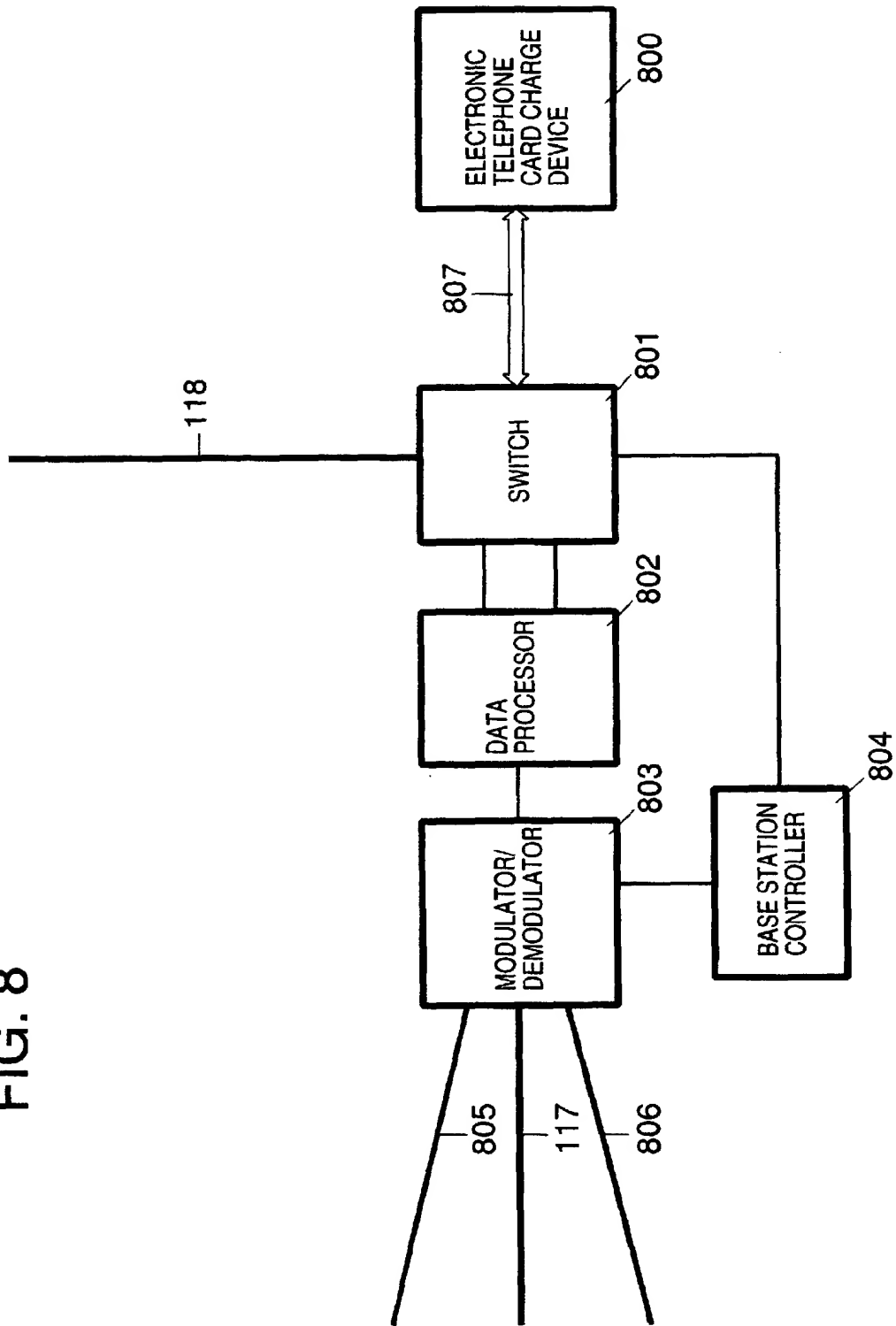


FIG. 8



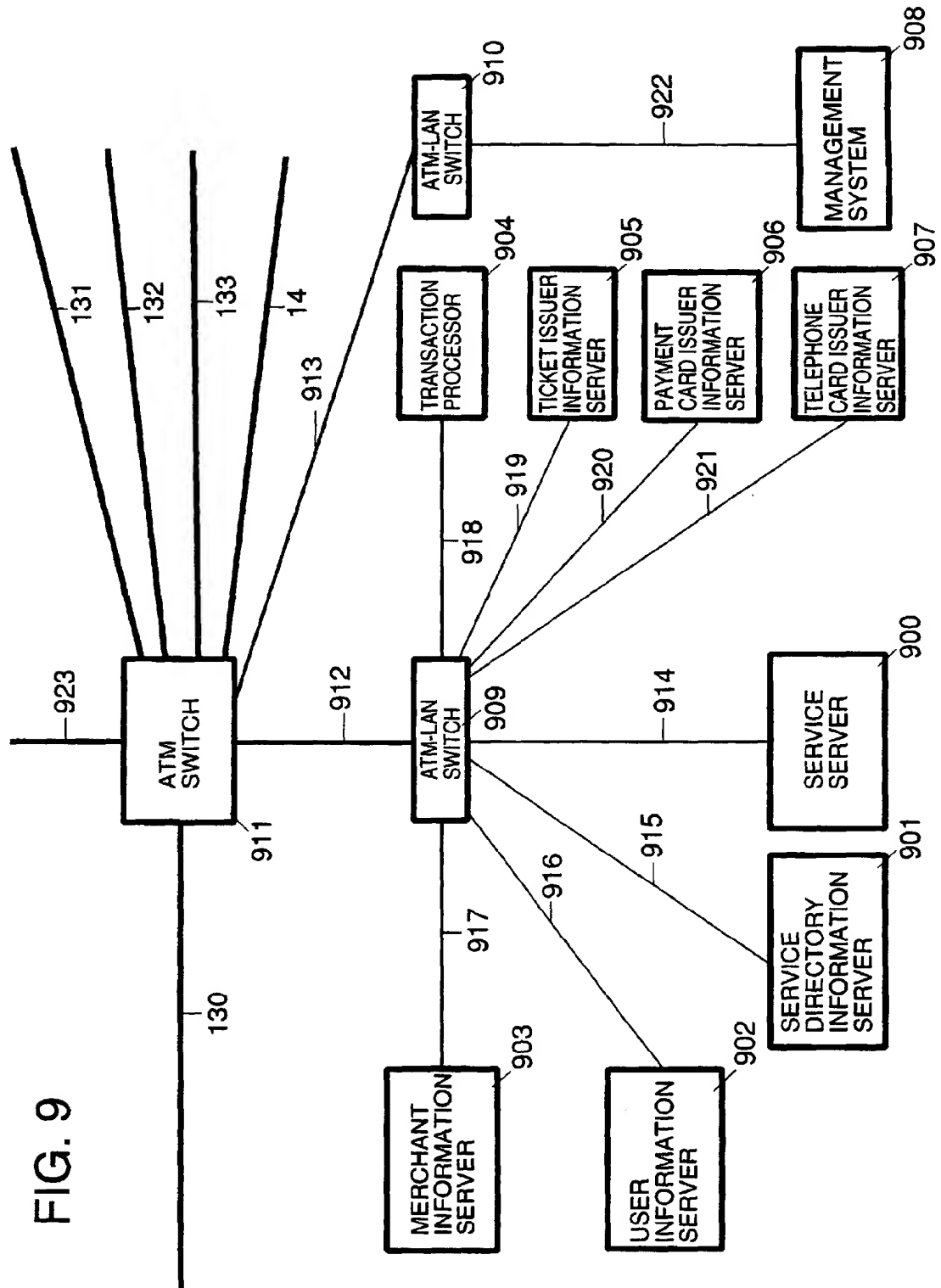


FIG. 10

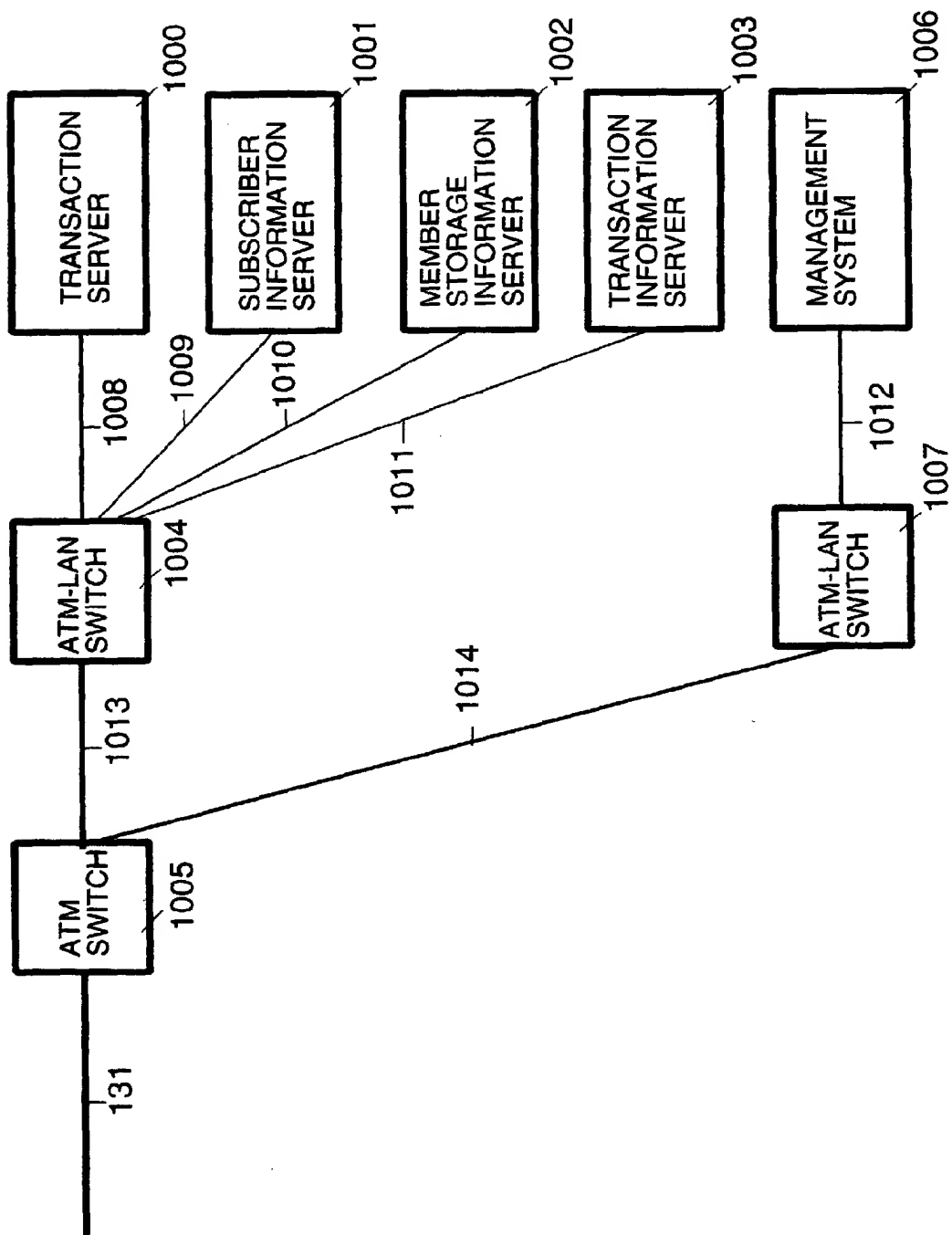


FIG. 11

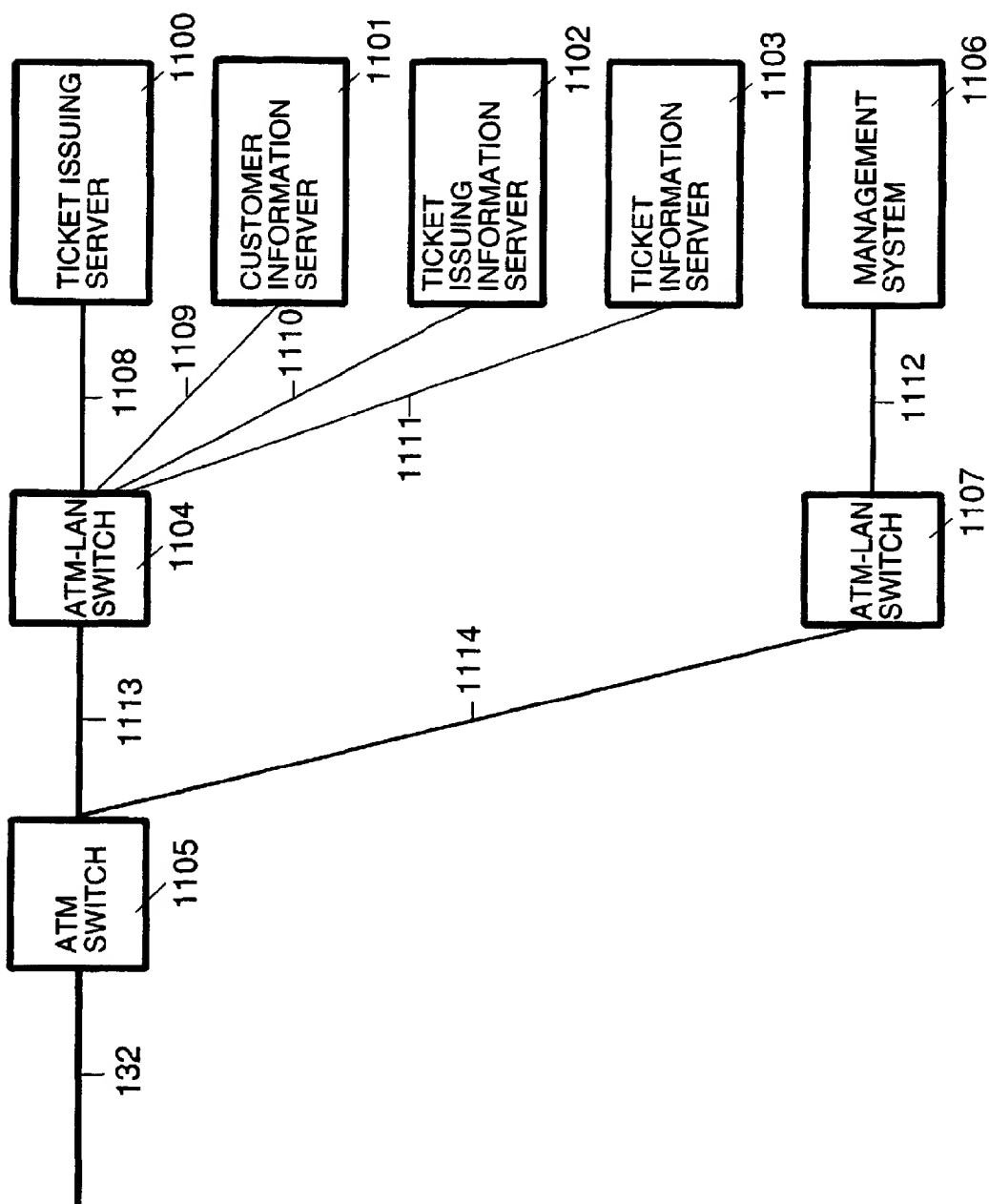


FIG. 12

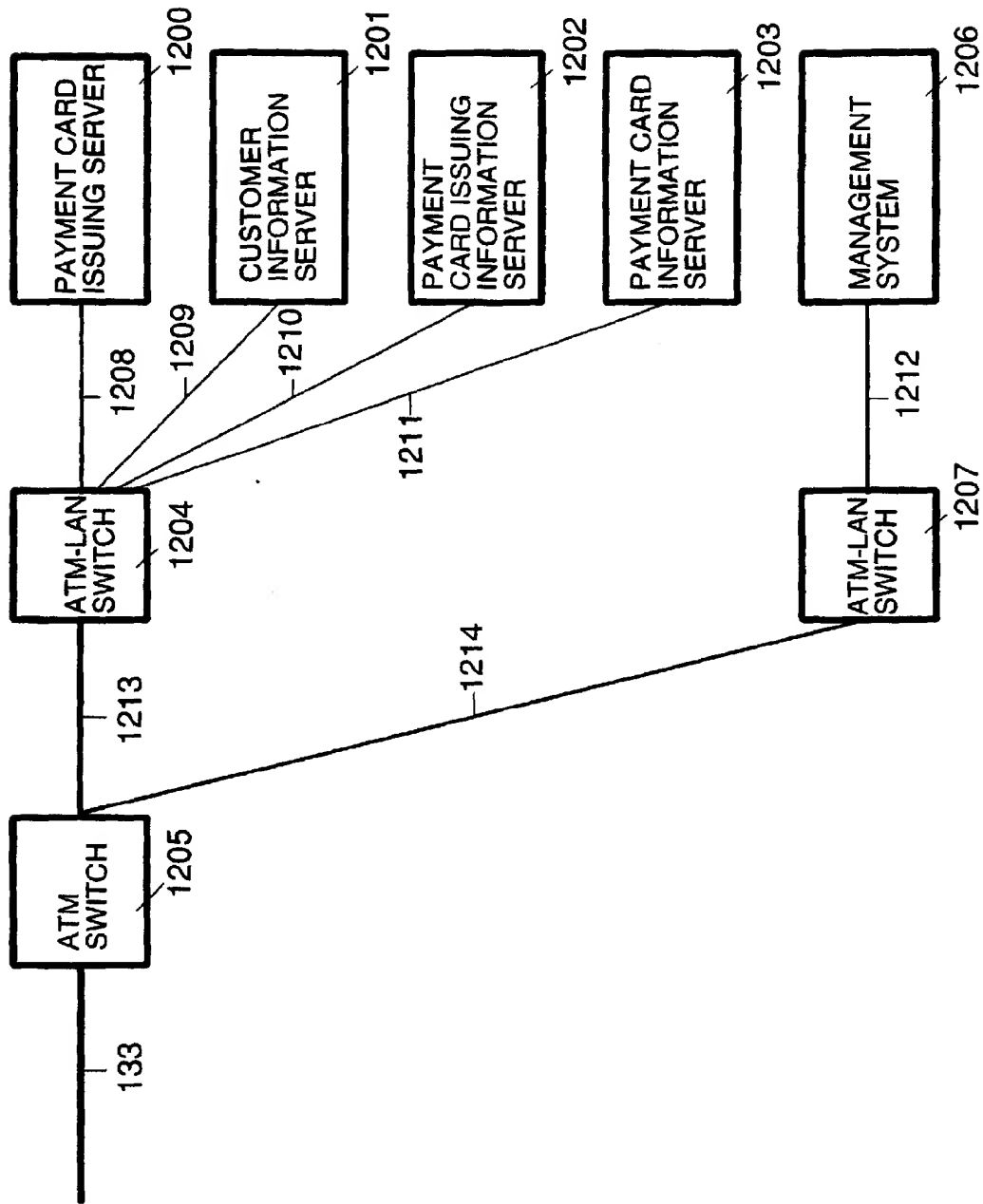


FIG. 13

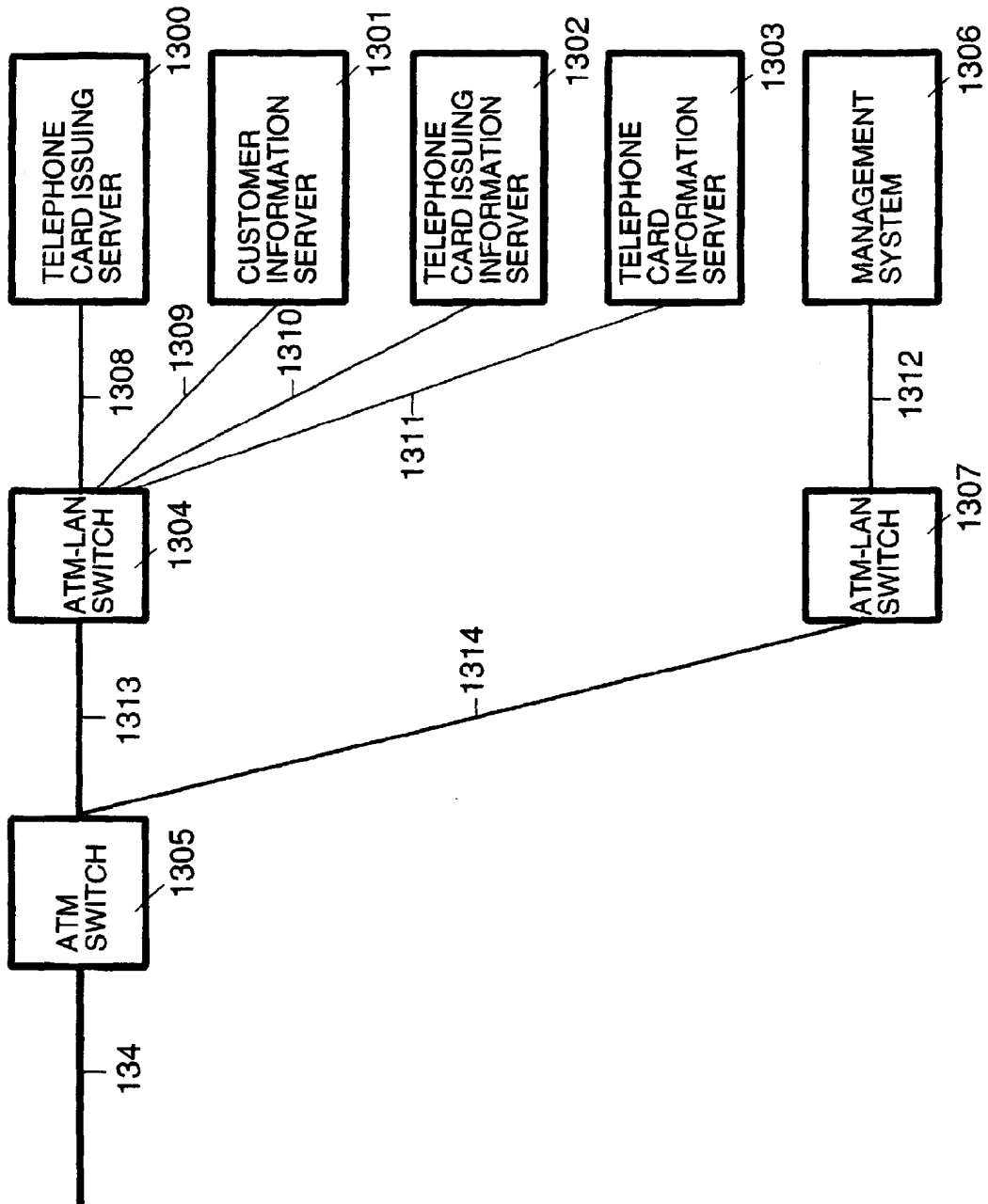


FIG. 14A

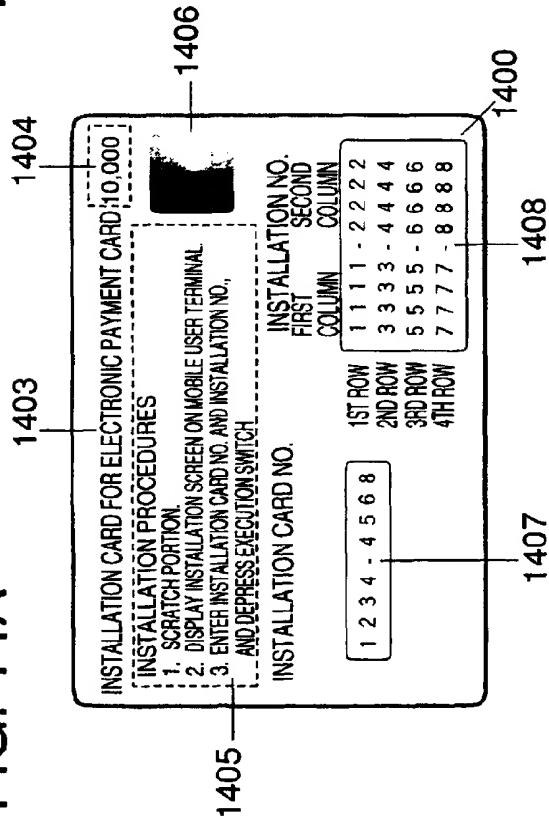


FIG. 14B

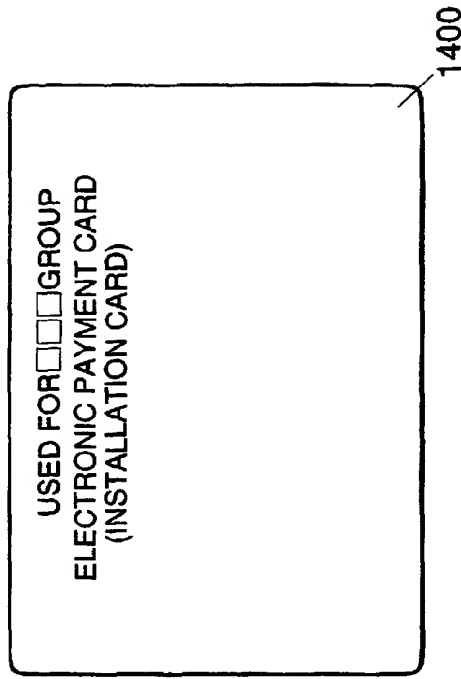


FIG. 14C

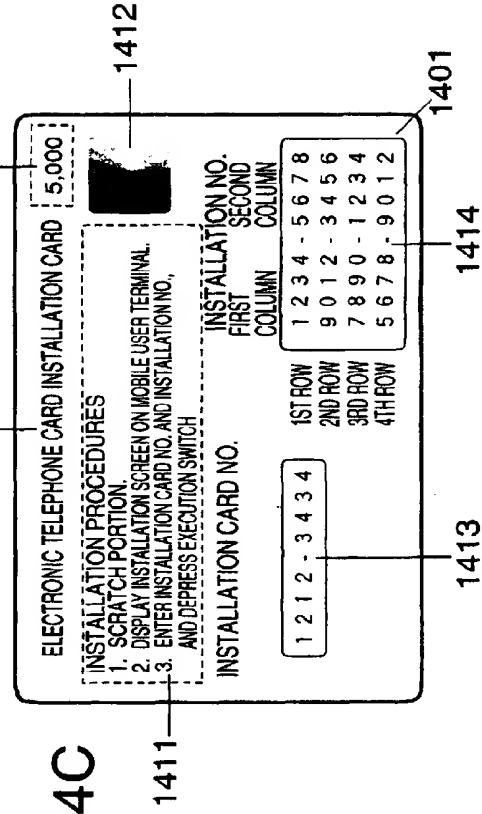


FIG. 14D

○○○ COMPANY

ON ○△□ CAMPAIGN

CALL FOR: TEL xxxx-xxxxxx

FIG. 14F

○○○□□ EXHIBITION

PERIOD : 2001/9/7 TO 9/30

TIME : 10:00 TO 17:00

PLACE : ○△□ MUSEUM

SPONSORED BY: △△△ NEWS COMPANY

CALL FOR : TEL xx-xxxx-xxxx

FIG. 14E

ELECTRONIC TICKET INSTALL CARD 2001.09.07

INSTALLATION PROCEDURES

1. SCRATCH PORTION.
2. DISPLAY INSTALLATION SCREEN ON MOBILE USER TERMINAL.
3. ENTER INSTALLATION CARD NO. AND INSTALLATION NO., AND DEPRESS EXECUTION SWITCH

INSTALLATION CARD NO.

1 2 1 2 - 7 8 7 8

INSTALLATION NO.

	FIRST COLUMN	SECOND COLUMN
1ST ROW	8 8 8 8	- 1 1 1 1
2ND ROW	6 6 6 6	- 3 3 3 3
3RD ROW	4 4 4 4	- 5 5 5 5
4TH ROW	2 2 2 2	- 7 7 7 7

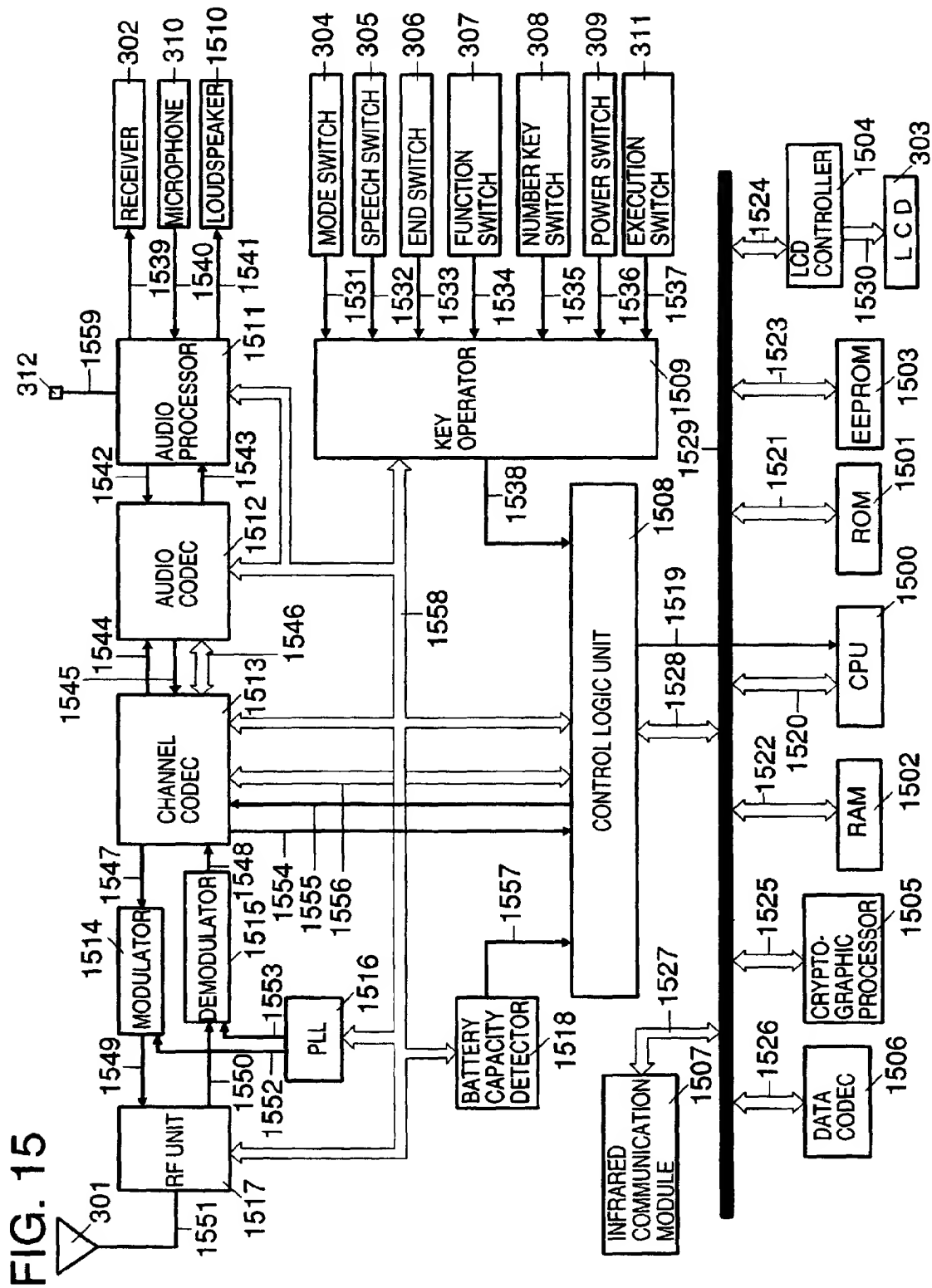


FIG. 16A

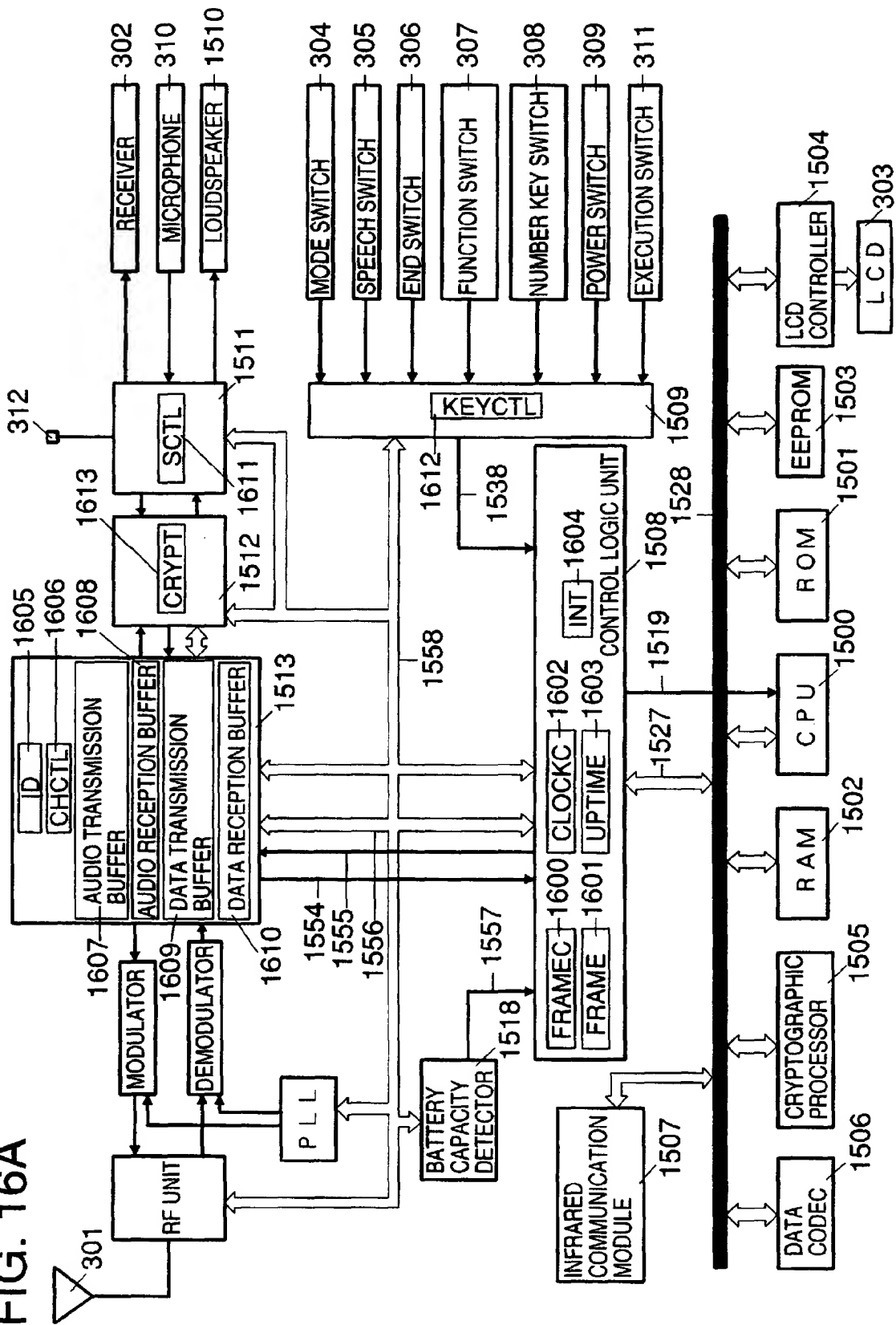


FIG. 16B

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
POWER DISPLAY	WIRELESS TELEPHONE DISPLAY	FRAME INTERRUPT	CALL RECEPTION INTERRUPT	DATA RECEPTION INTERRUPT	UPDATE INTERRUPT	BATTERY INTERRUPT	KEY INTERRUPT				"END"	"SPEECH"	"MODE"	"EXECUTE"	"POWER"
INT															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
"F 4"	"F 3"	"F 2"	"F 1"	"#"	"*"	"9"	"8"	"7"	"6"	"5"	"4"	"3"	"2"	"1"	"0"
INT															

FIG. 17

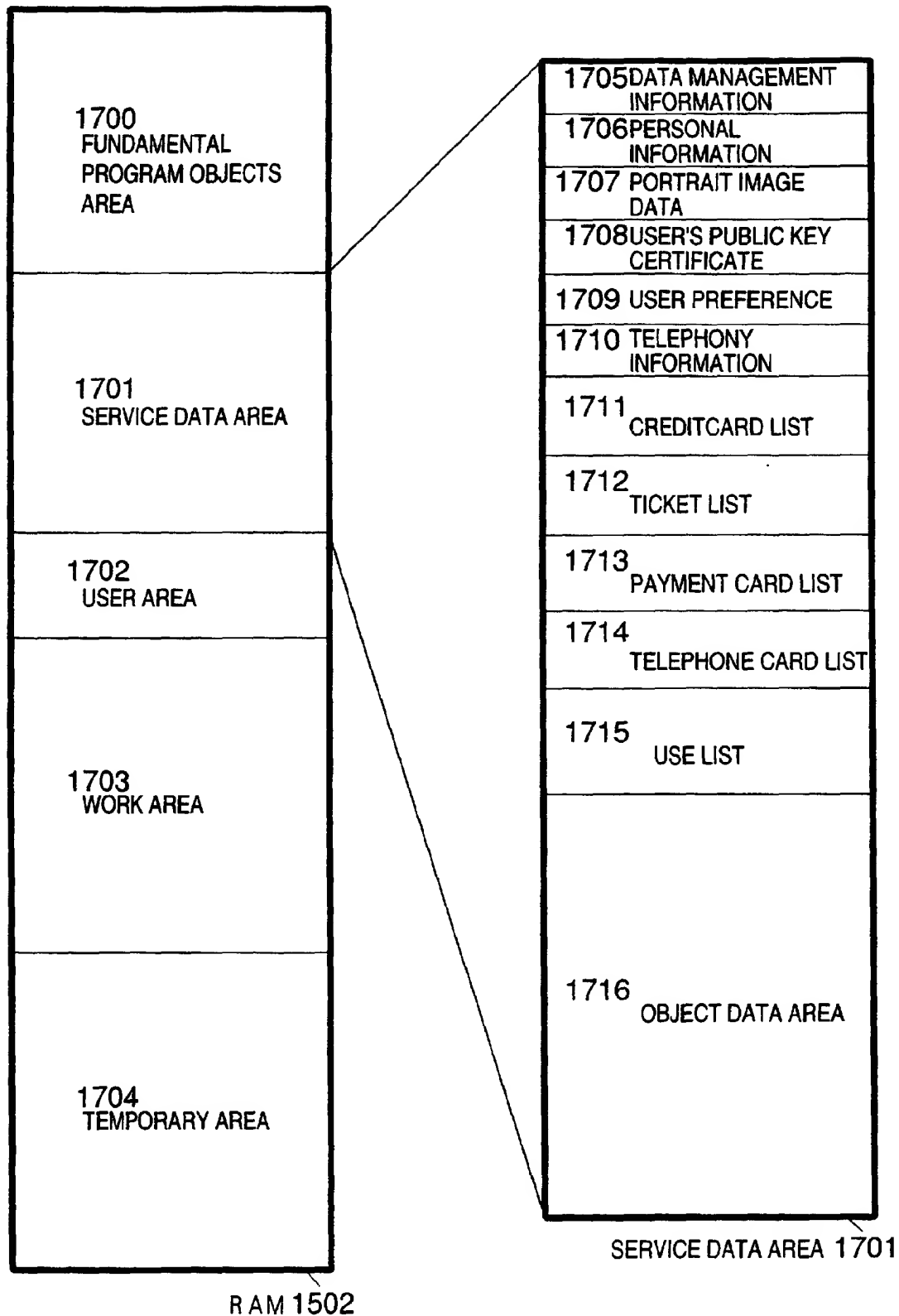


FIG. 18

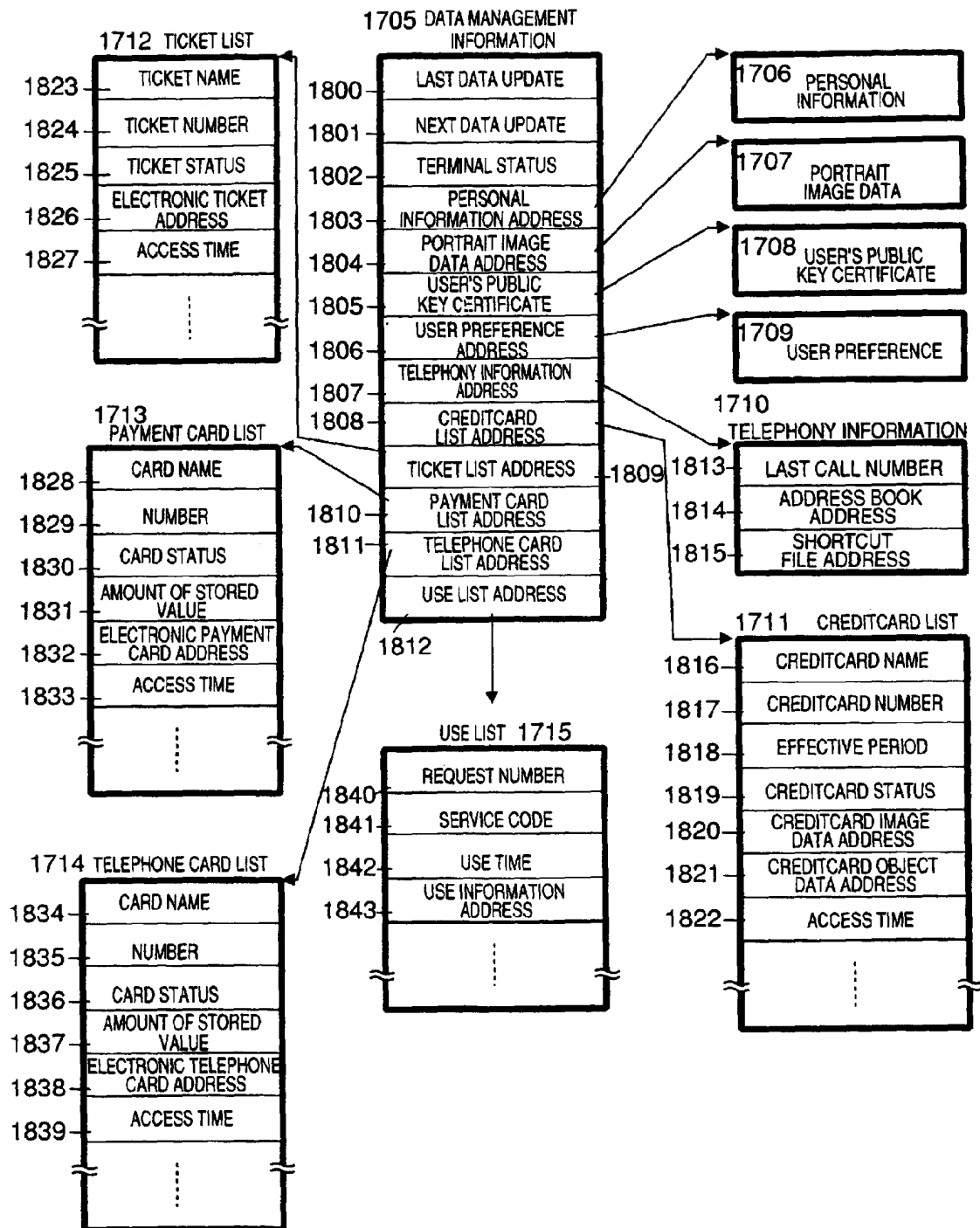


FIG. 19

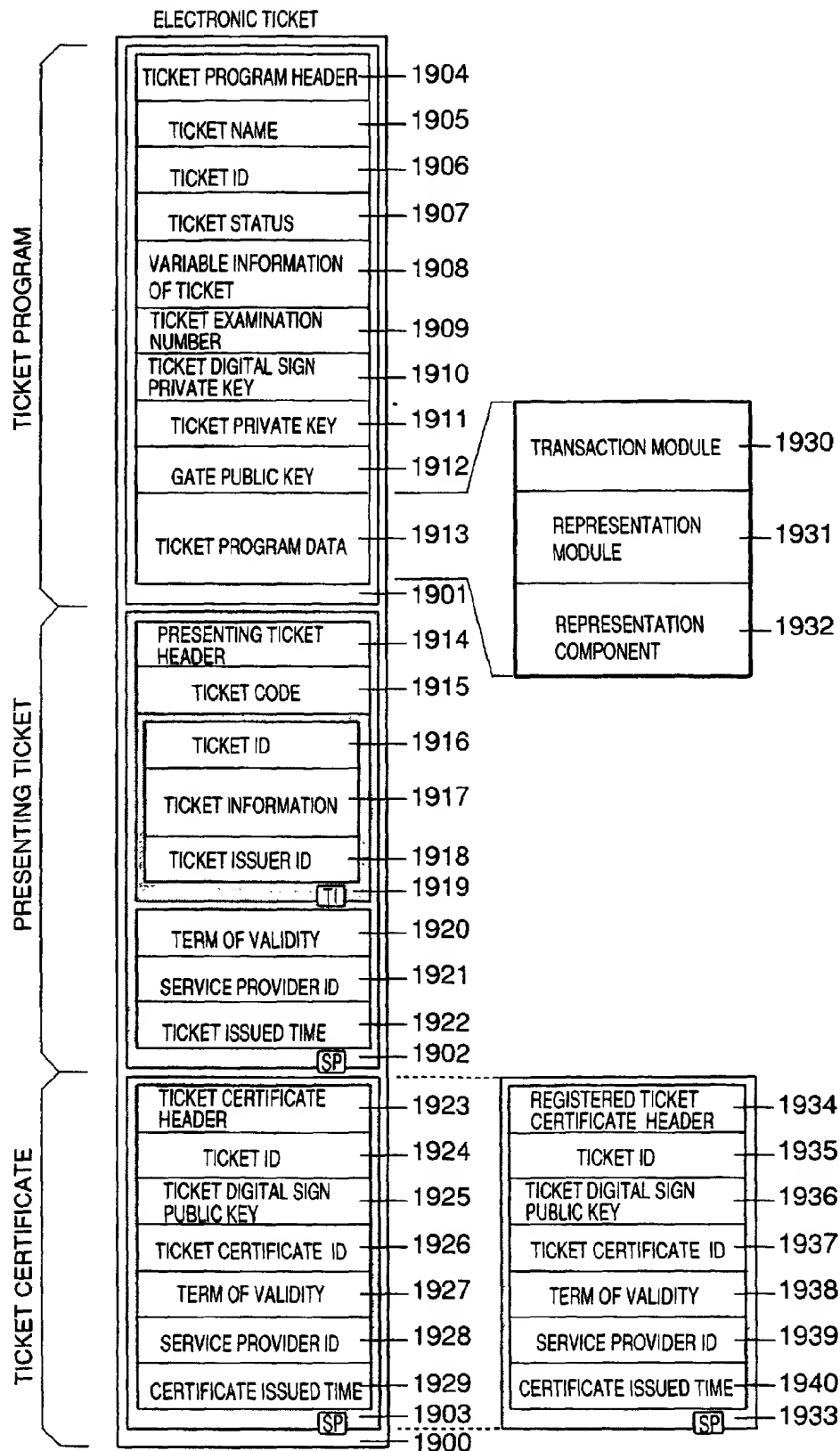


FIG. 20

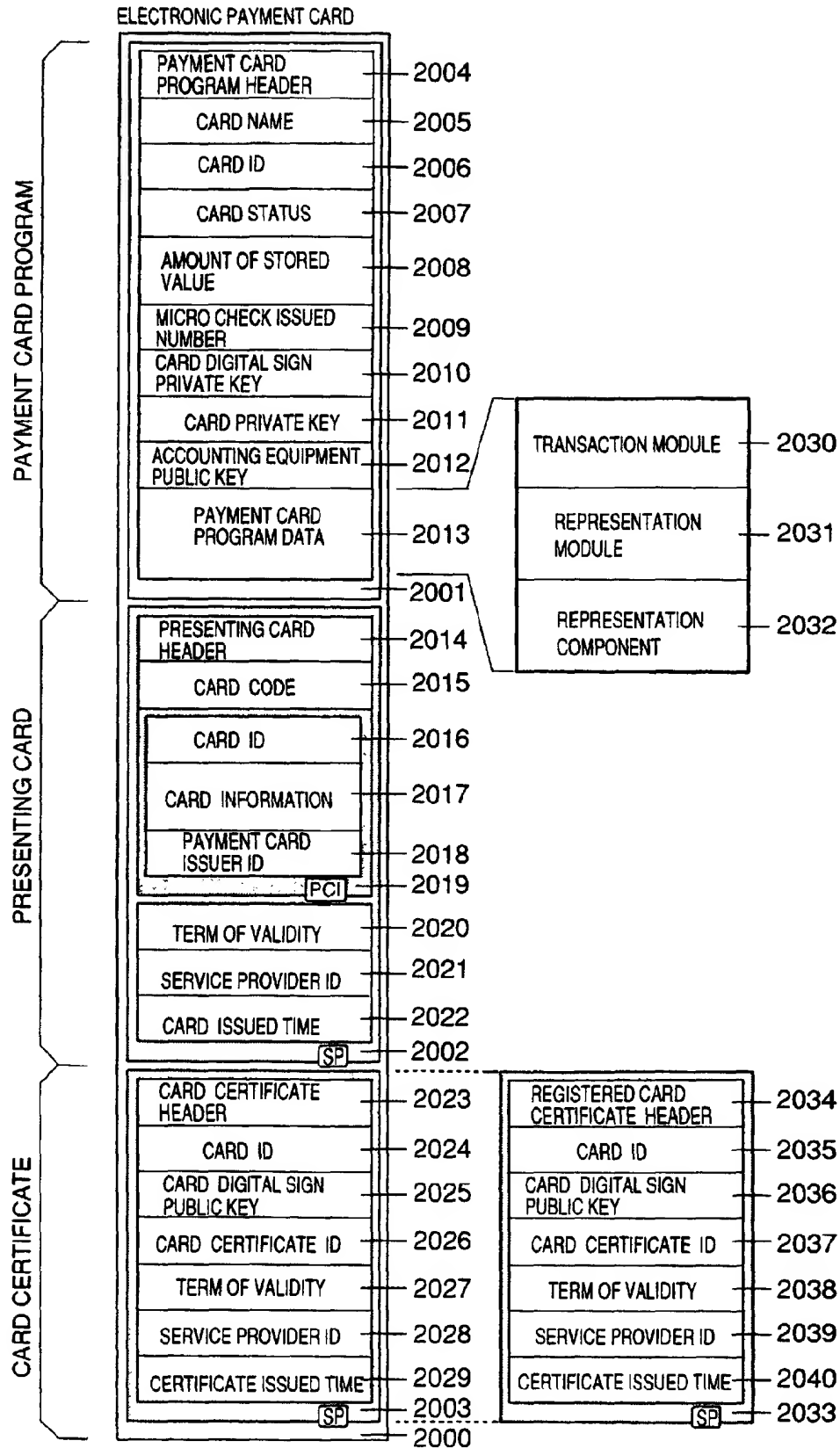
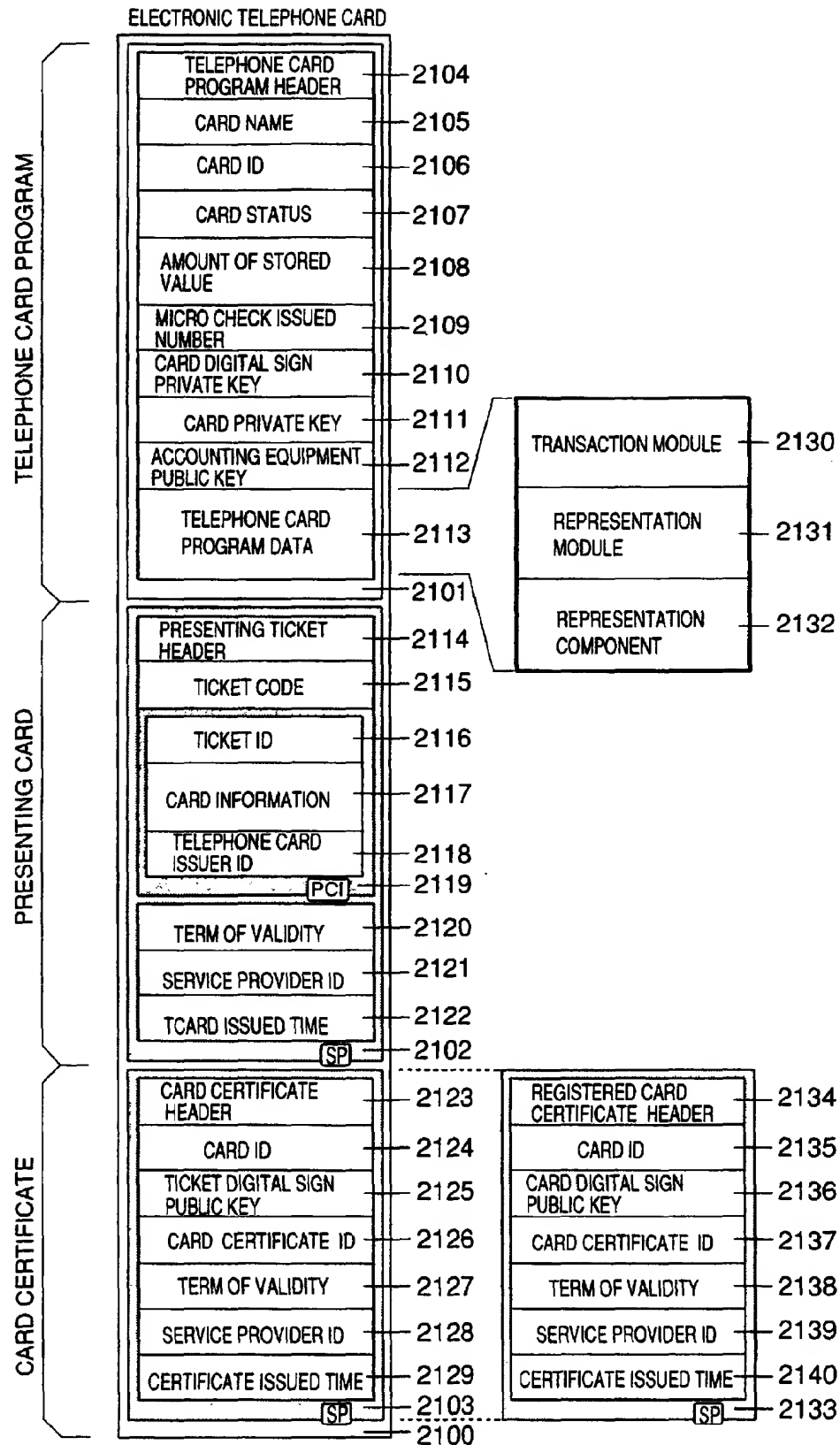
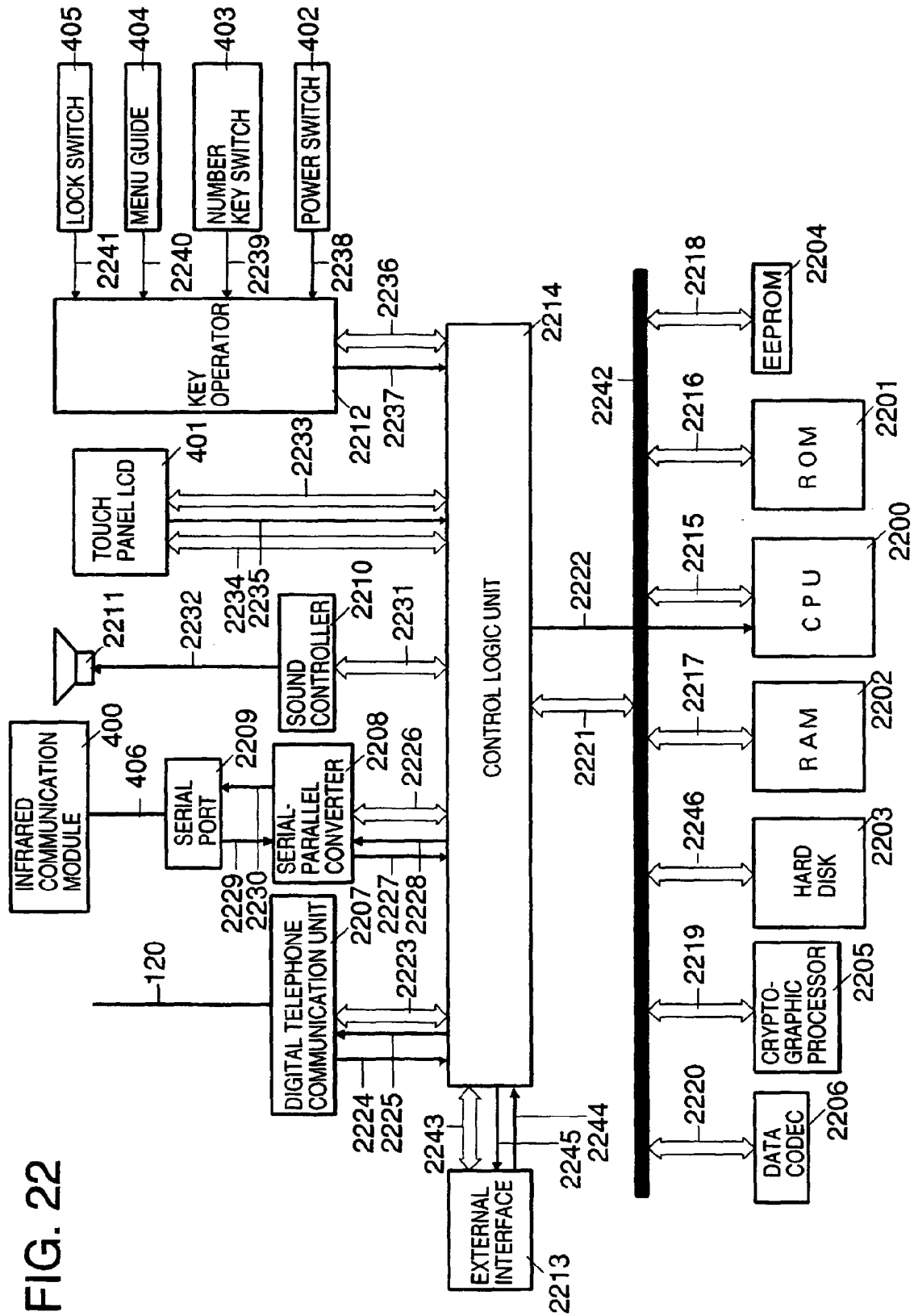


FIG. 21





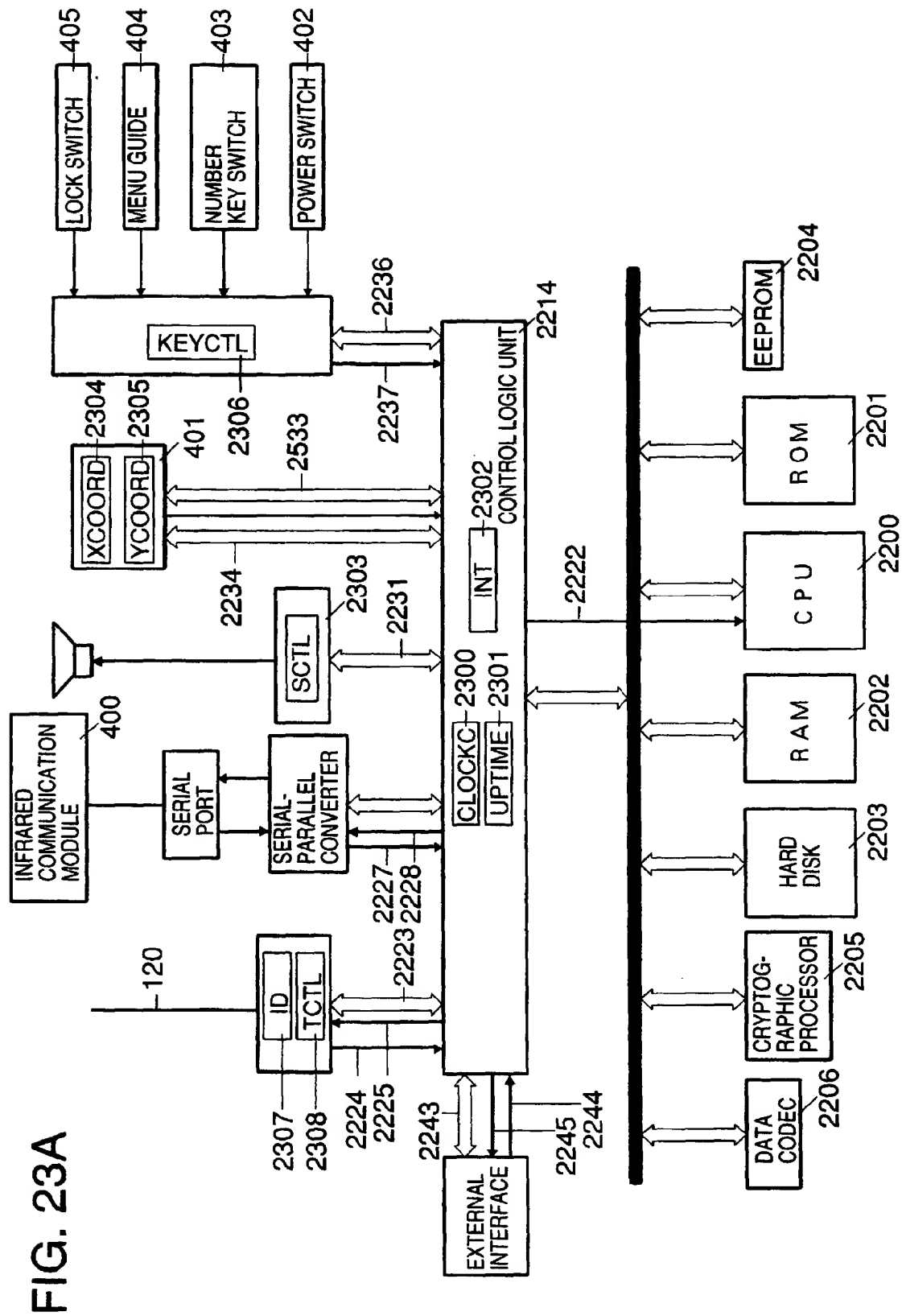


FIG. 23B

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
POWER DISPLAY	PHONE SPEECH DISPLAY	TOUCH PANEL INTERRUPT	INFRARED RECEPTION INTERRUPT	DATA RECEPTION INTERRUPT	UPDATE INTERRUPT	EXTERNAL IF INTERRUPT	KEY INTERRUPT						"MENU"	"LOCK"	"POWER"
INT															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
"F 4"	"F 3"	"F 2"	"F 1"	"#"	"*"	"9"	"8"	"7"	"6"	"5"	"4"	"3"	"2"	"1"	"0"
INT															

FIG. 24

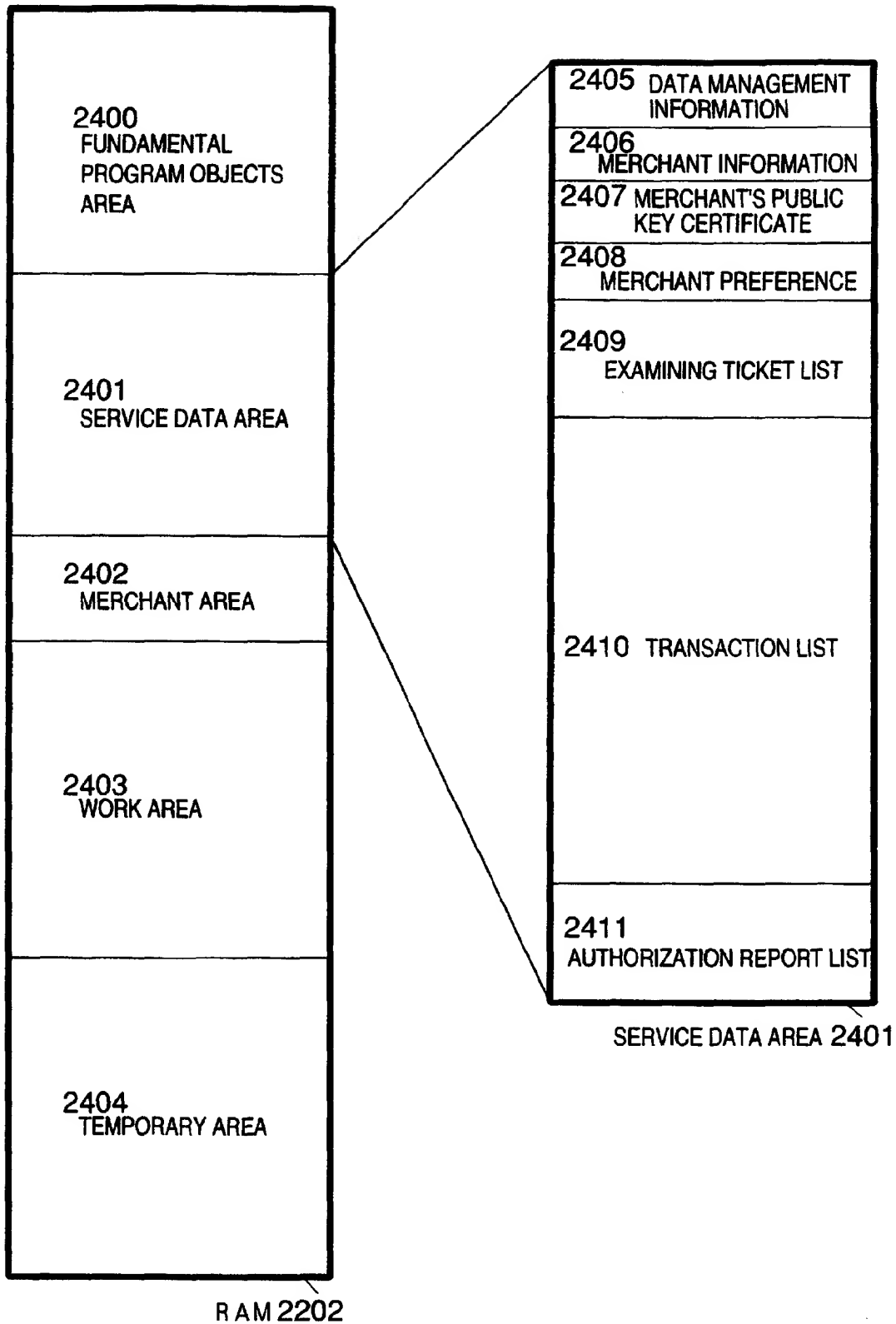


FIG. 25

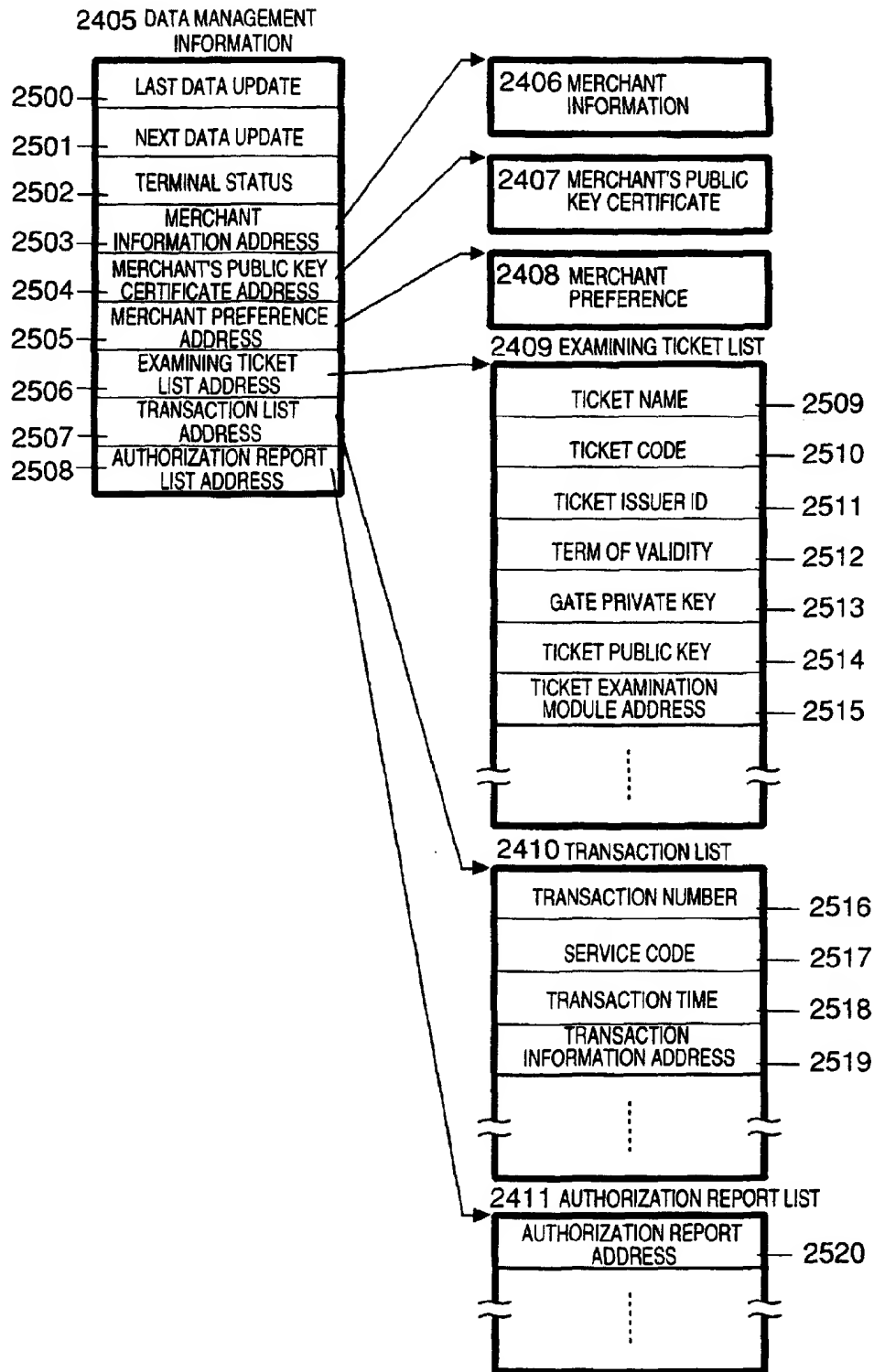


FIG. 26

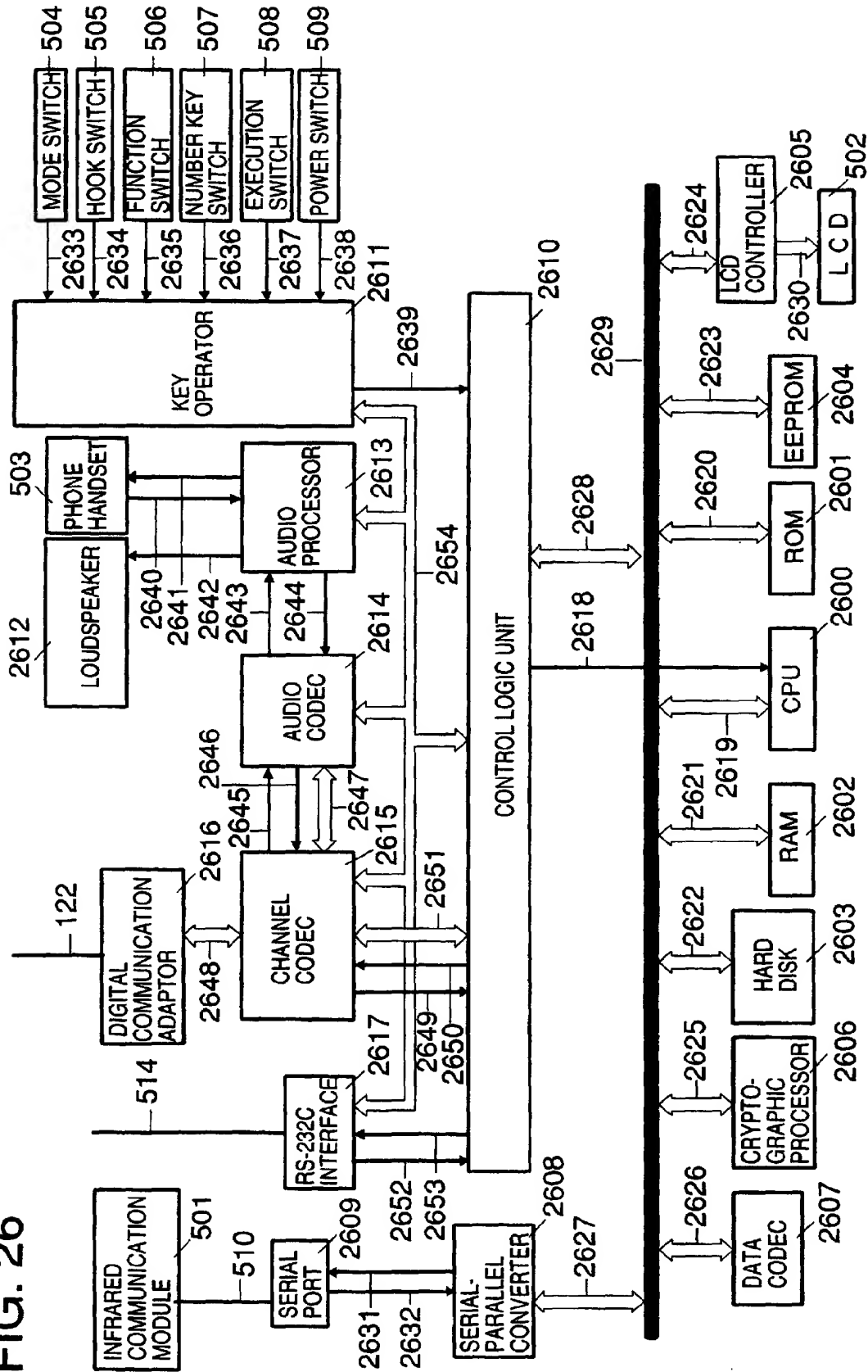


FIG. 27A

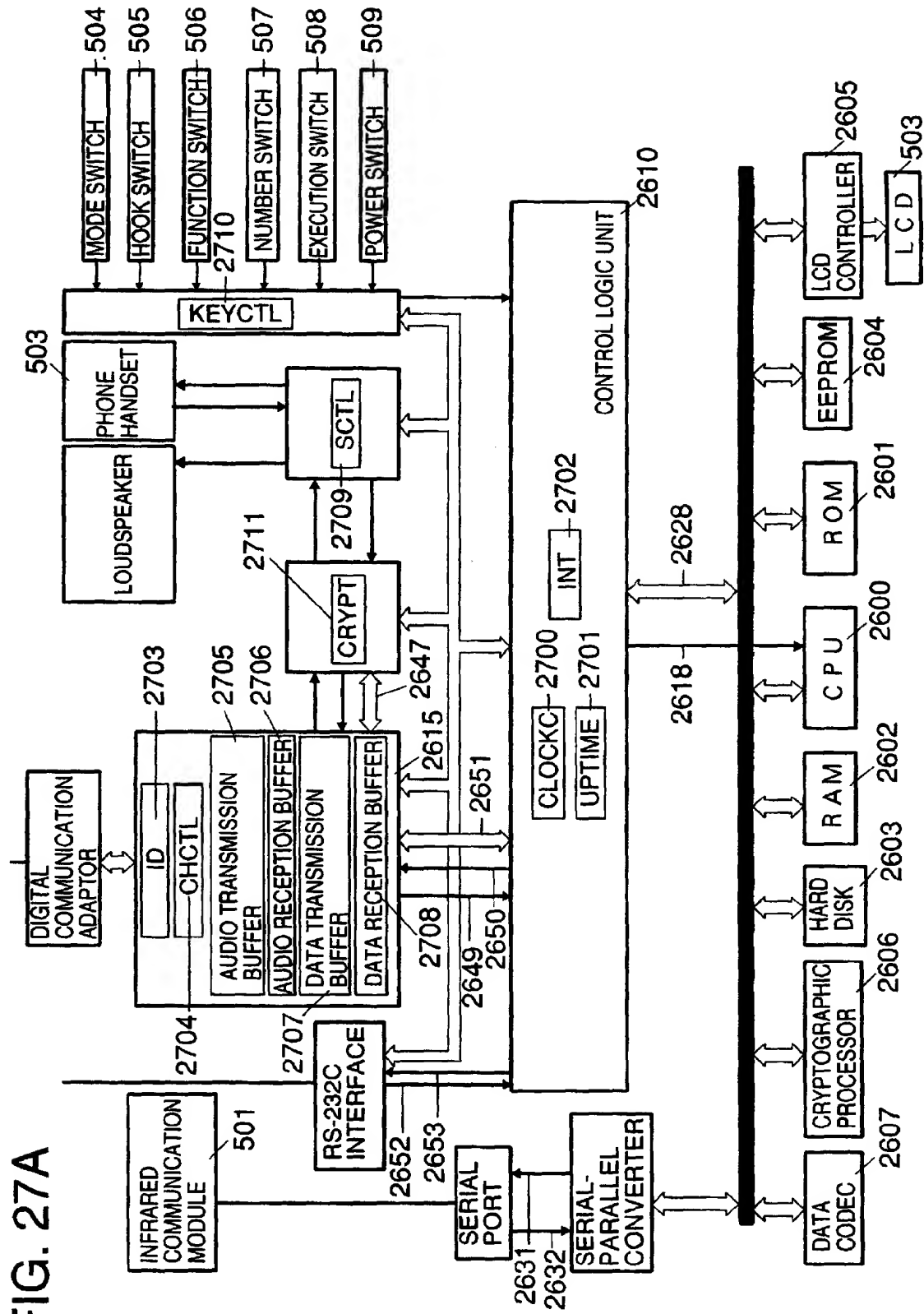


FIG. 27B

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
POWER DISPLAY	TELEPHONE DISPLAY		CALL RECEPTION INTERRUPT	DATA RECEPTION INTERRUPT	UPDATE INTERRUPT	EXTERNAL IF INTERRUPT	KEY INTERRUPT				"HOOK"		"MODE"	"EXECUTE"	"POWER"
INT															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
"F 4 "	"F 3 "	"F 2 "	"F 1 "	"# "	"* "	"9 "	"8 "	"7 "	"6 "	"5 "	"4 "	"3 "	"2 "	"1 "	"0 "
INT															

FIG. 28

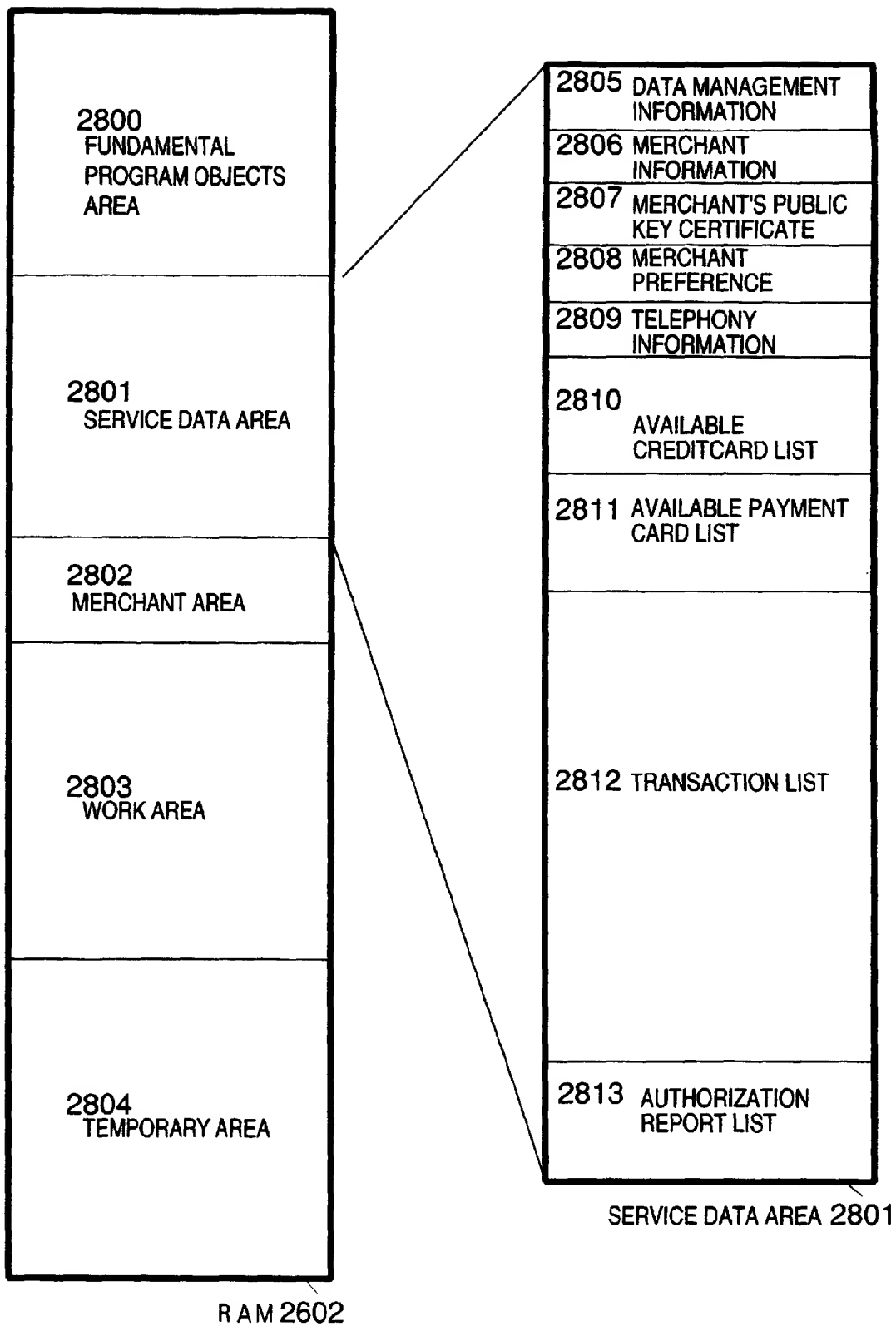


FIG. 29

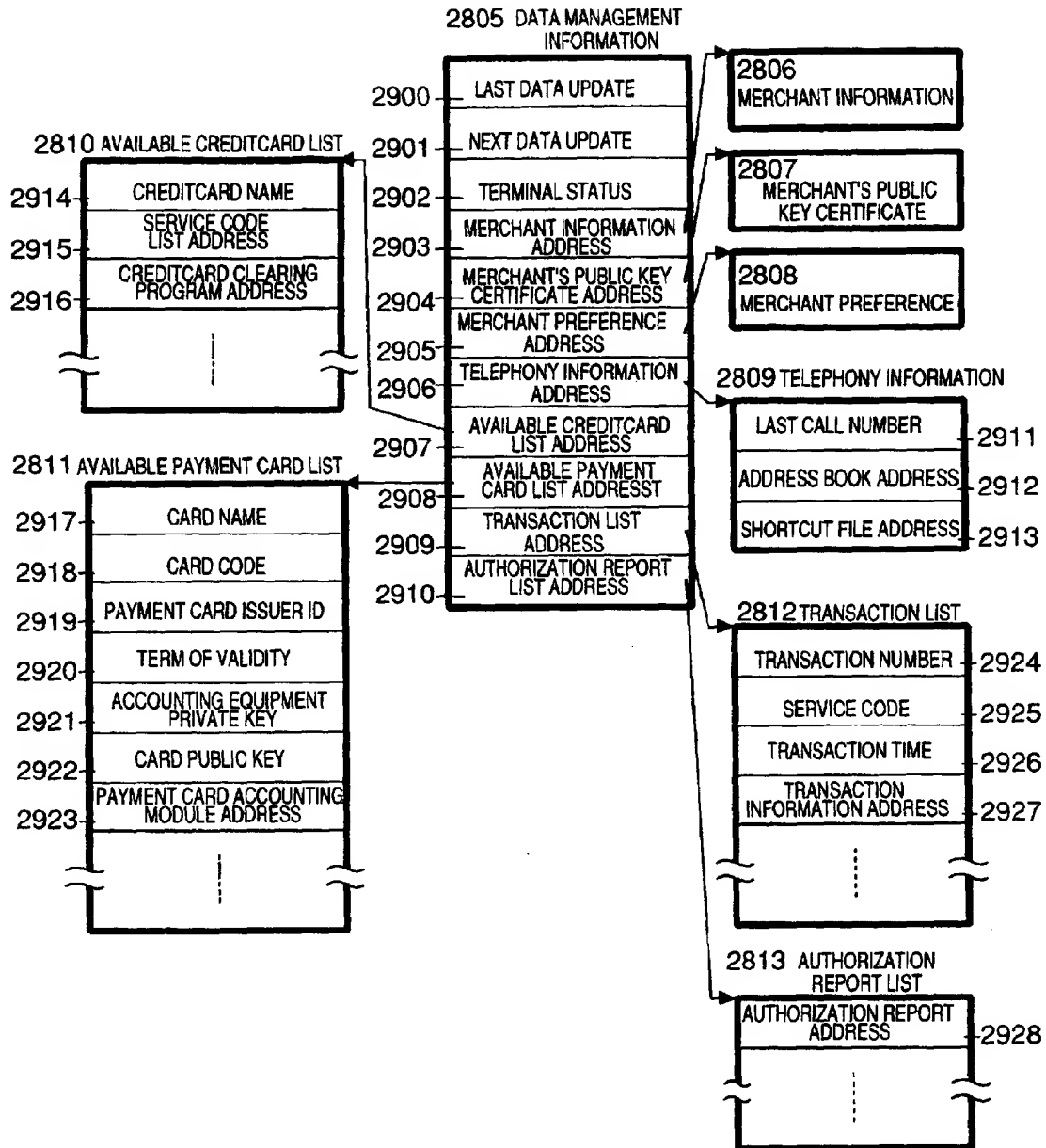


FIG. 30

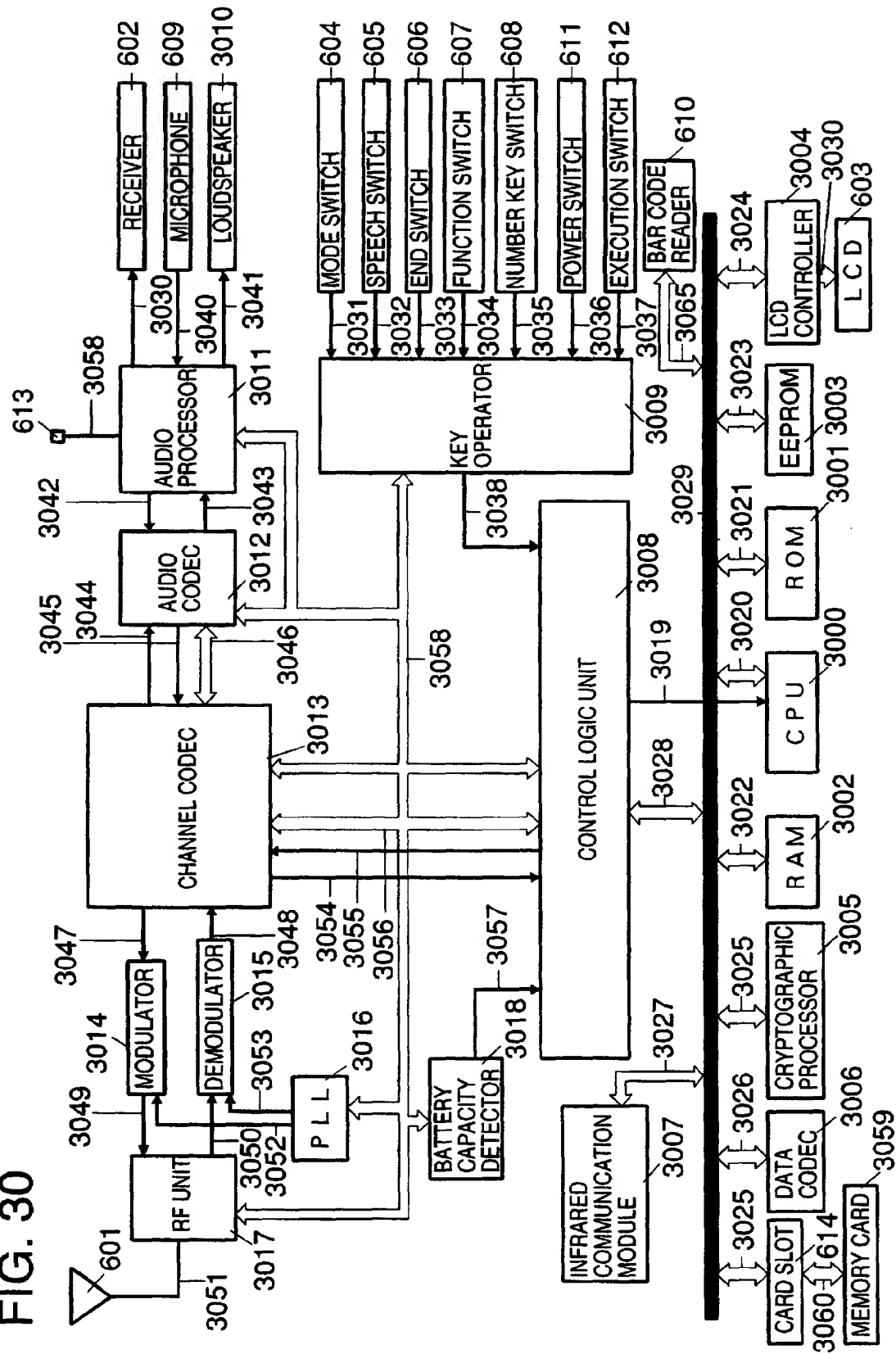


FIG. 31A

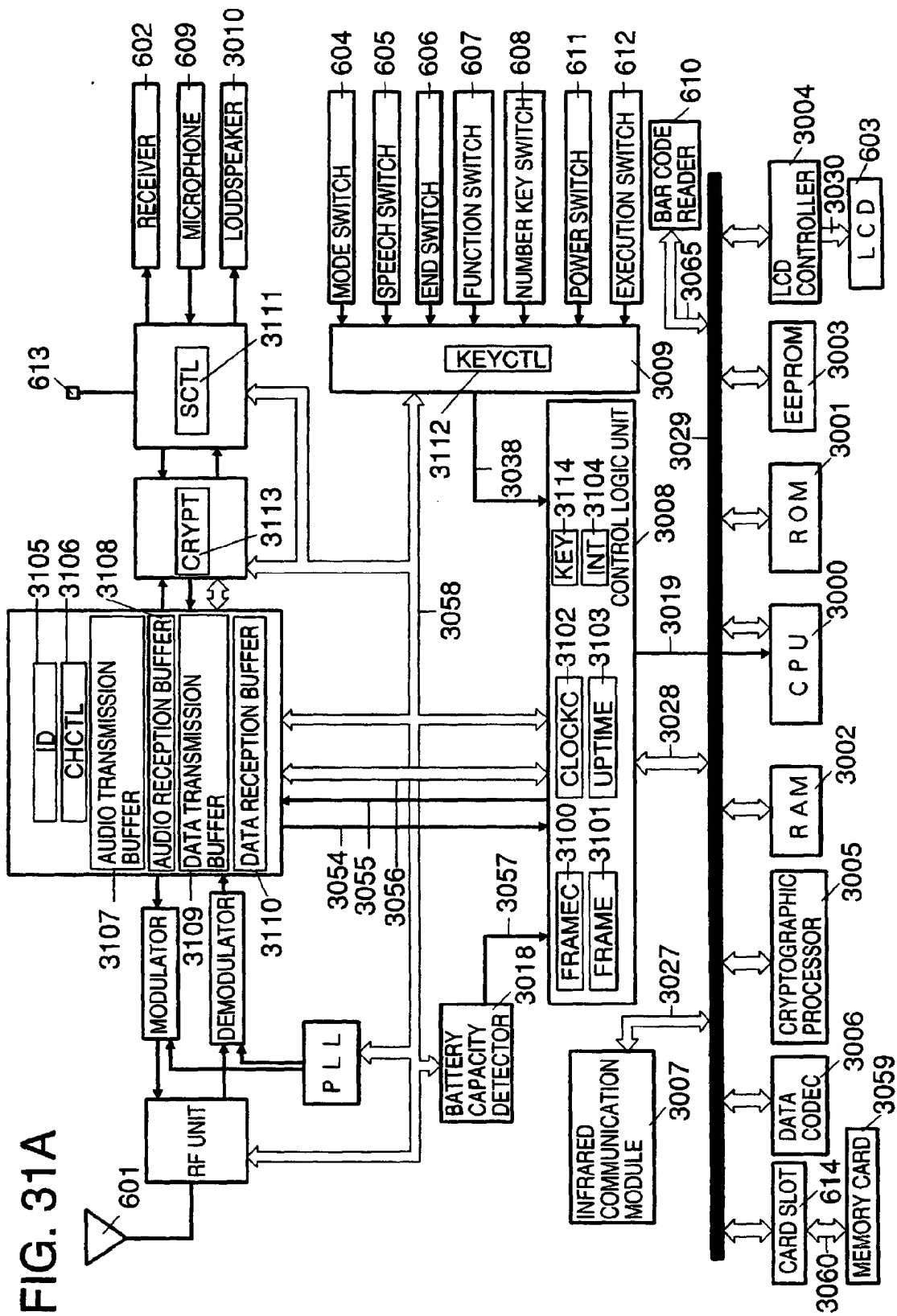


FIG. 31B

	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
INT	POWER DISPLAY	WIRELESS TELEPHONE DISPLAY	FRAME INTERRUPT	CALL RECEPTION INTERRUPT	DATA RECEPTION INTERRUPT	UPDATE INTERRUPT	BATTERY INTERRUPT	KEY INTERRUPT								

FIG. 31C

	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
KEY	"="	"+"	"—"	"X"	"÷"	"."	"SUM"					"END"	"SPEECH"	"MODE"	"EXECUTE"	"POWER"
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
KEY	"F 4"	"F 3"	"F 2"	"F 1"	"#"	"*"	"9"	"8"	"7"	"6"	"5"	"4"	"3"	"2"	"1"	"0"

FIG. 32

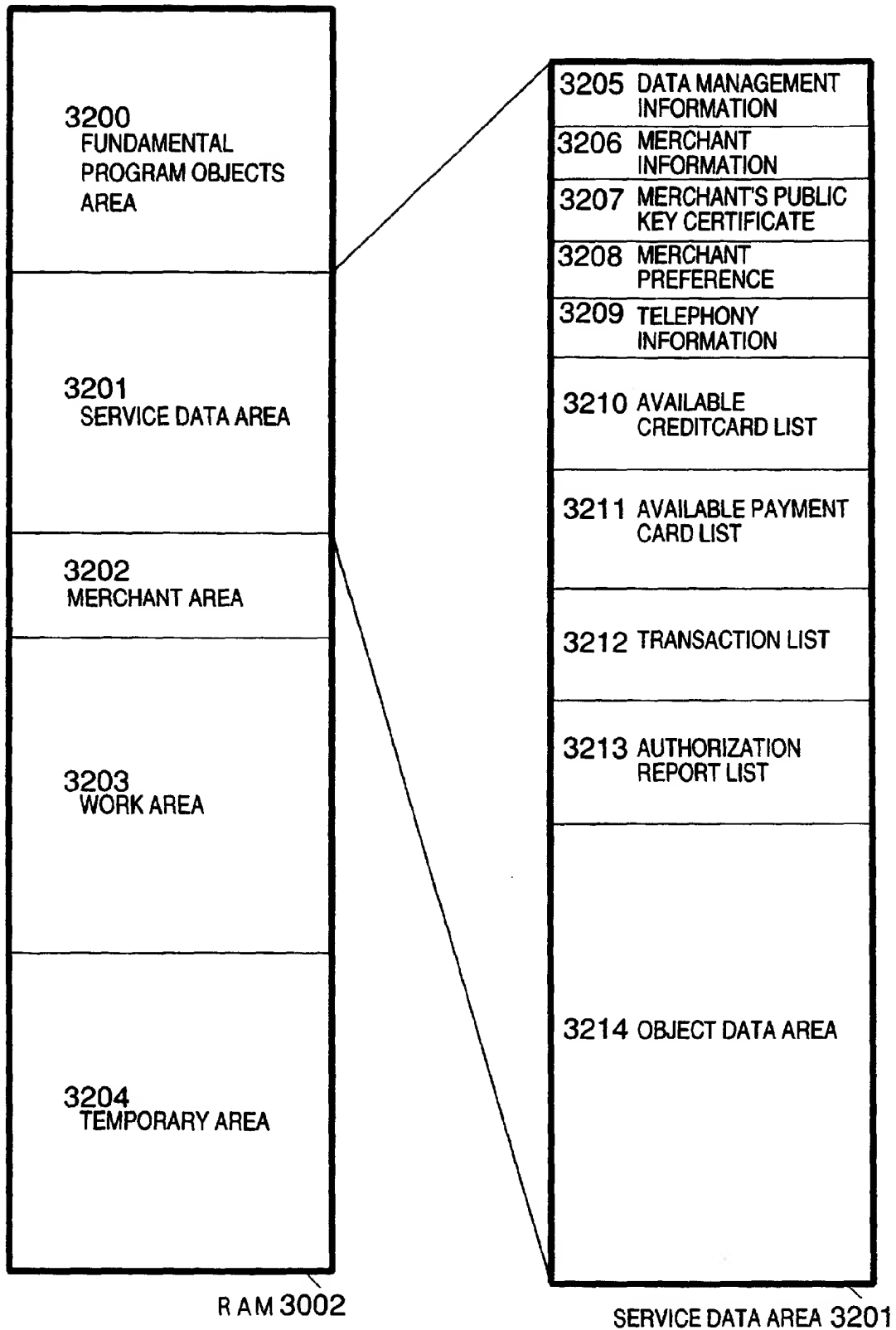


FIG. 33

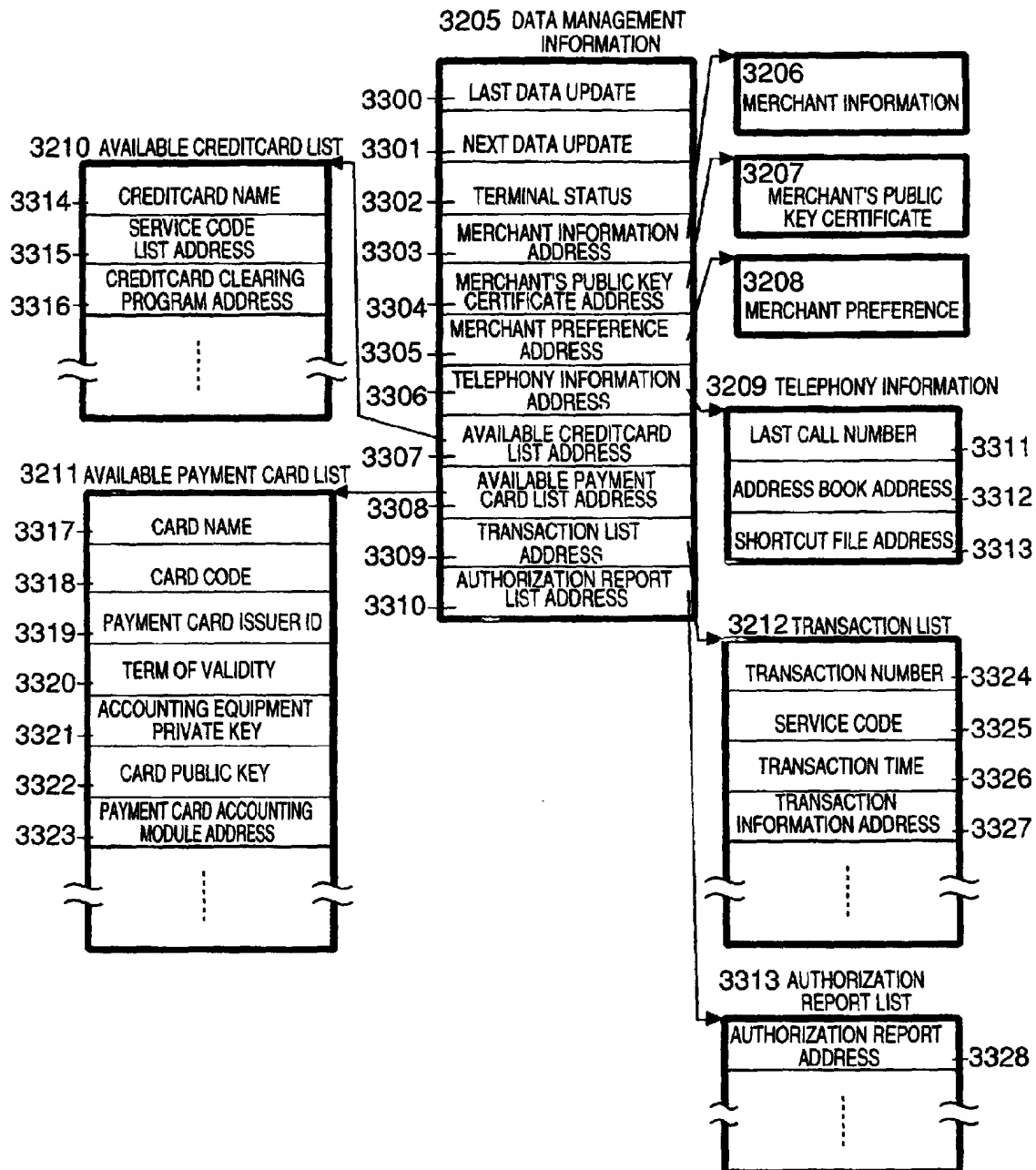


FIG. 34

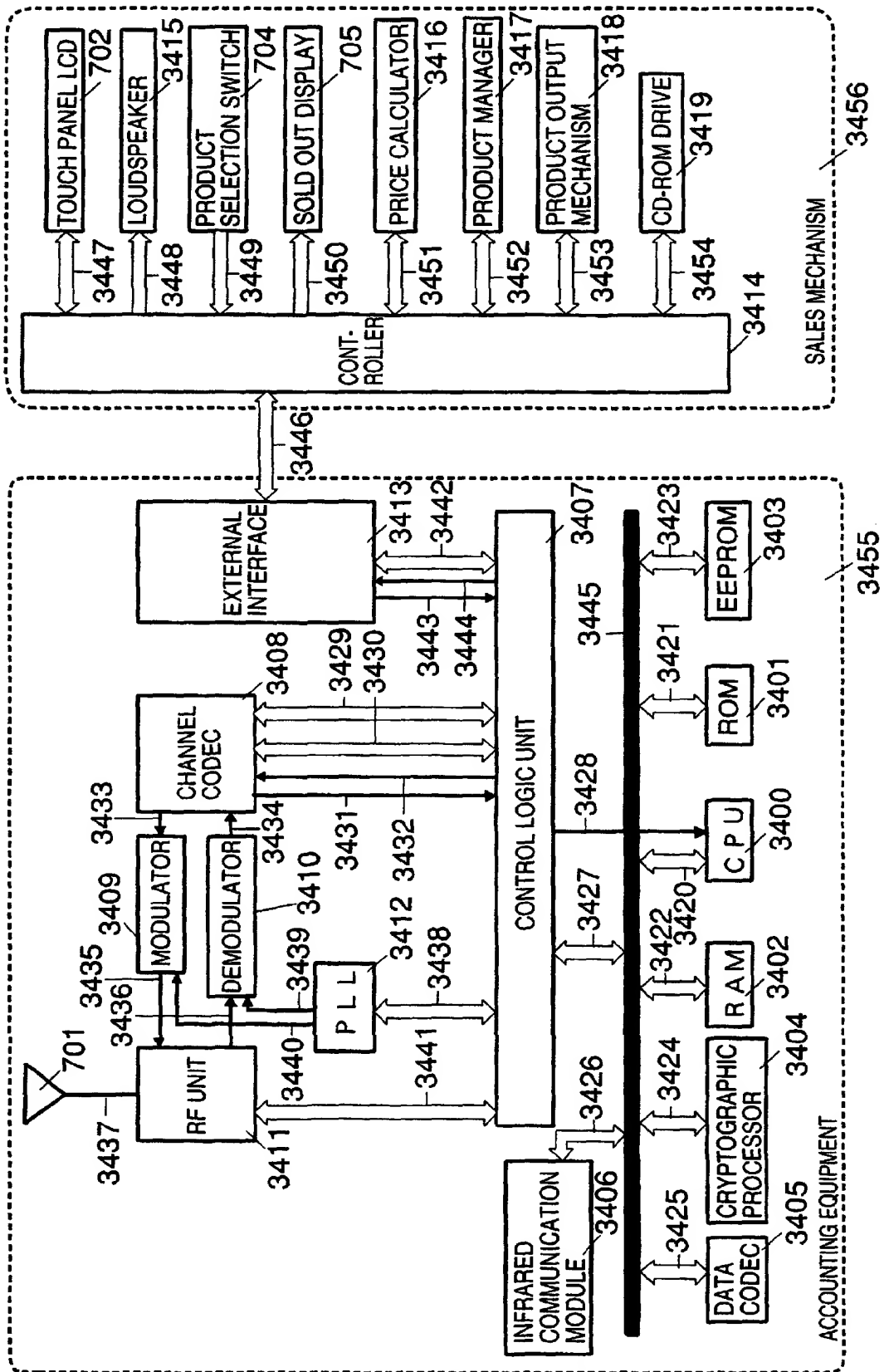


FIG. 35A

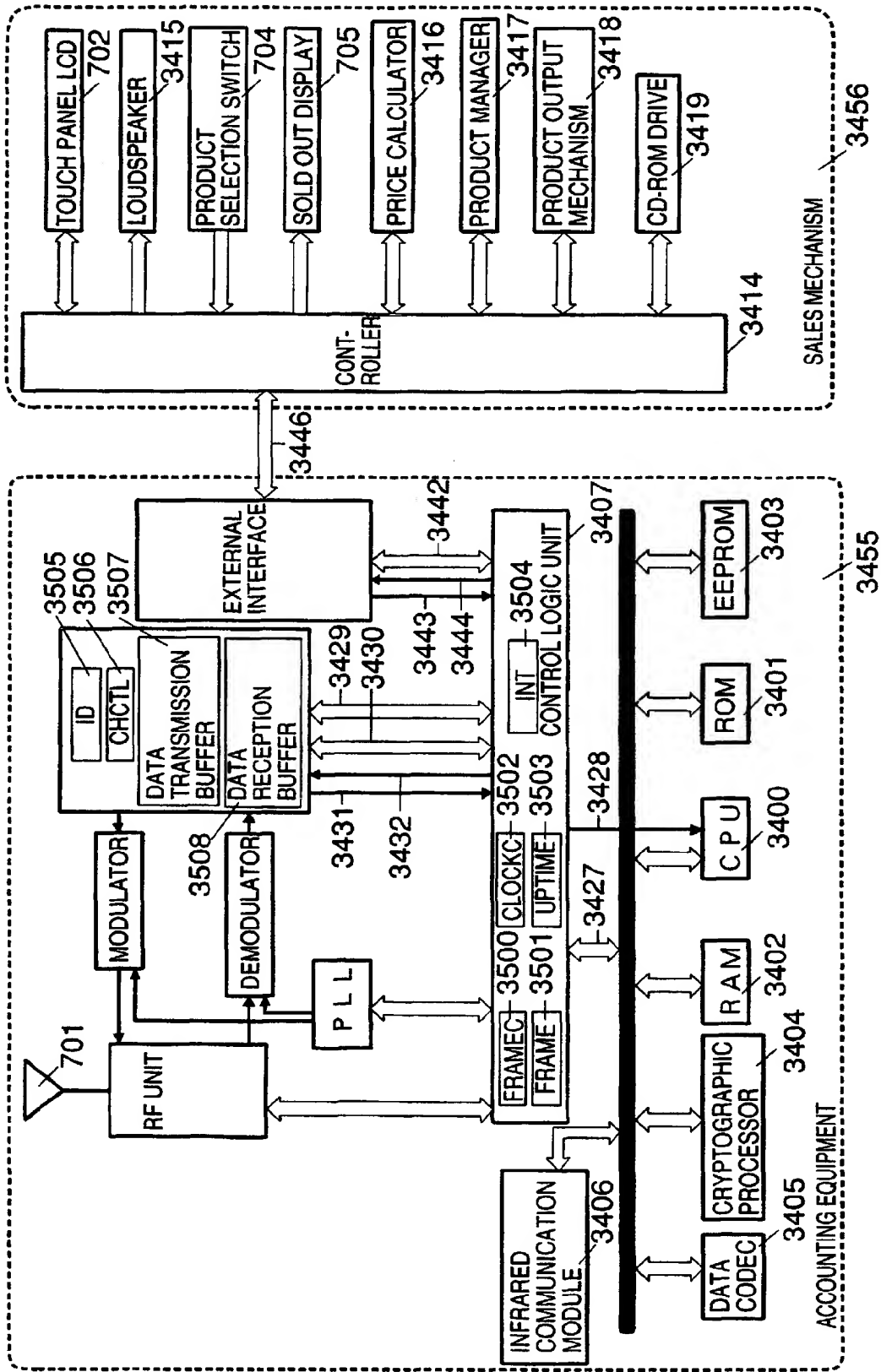


FIG. 35B

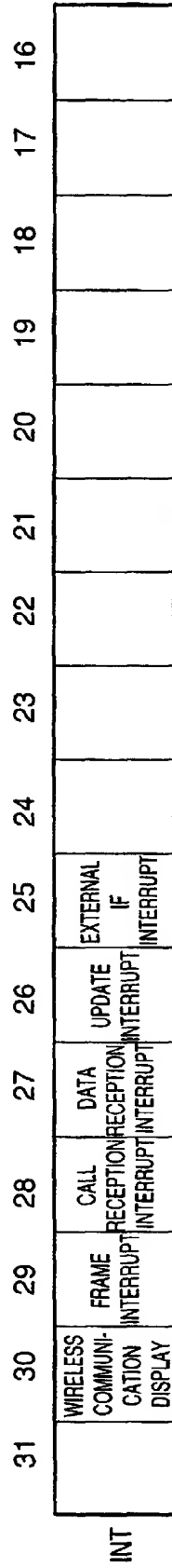


FIG. 36

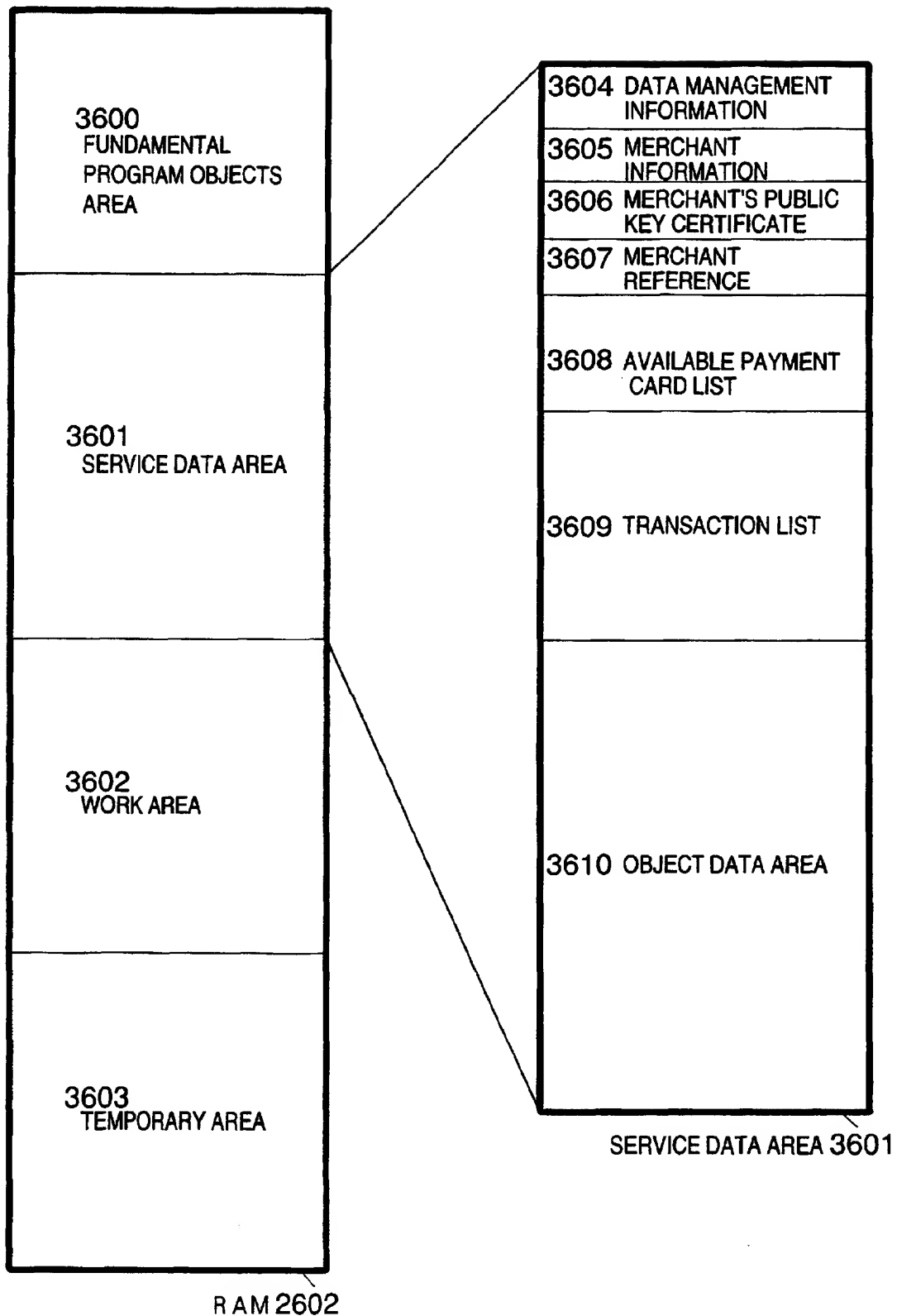


FIG. 37

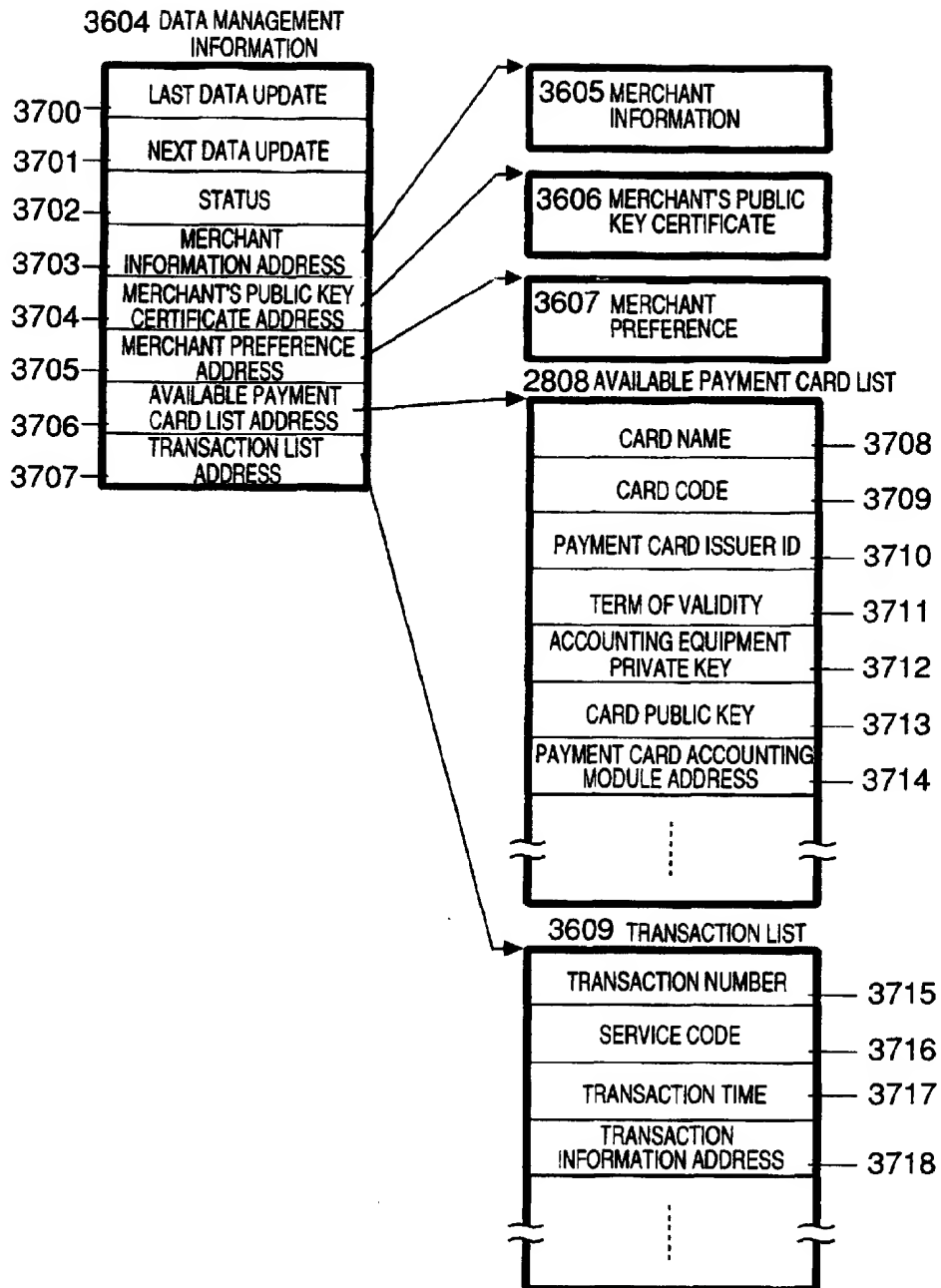


FIG. 38

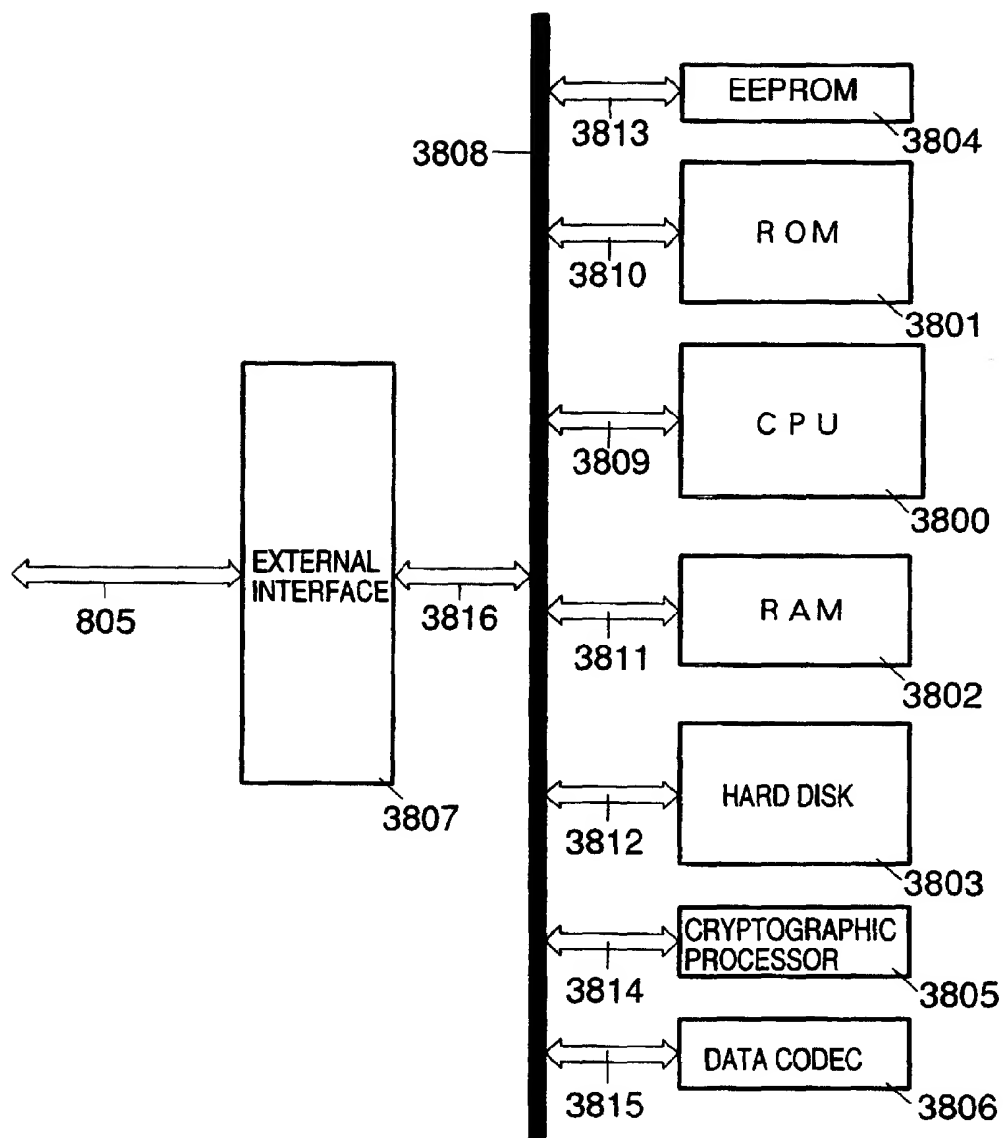


FIG. 39

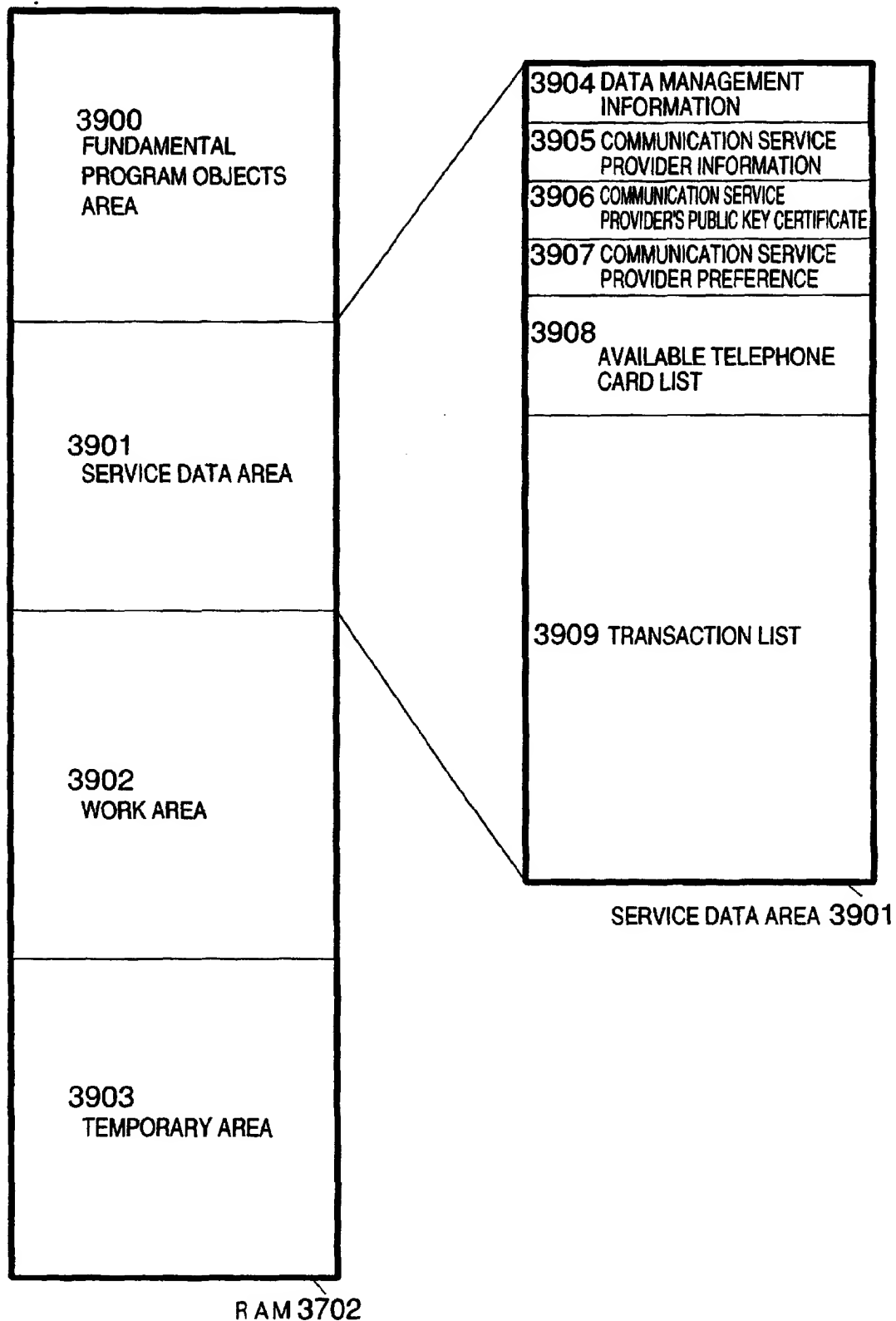


FIG. 40

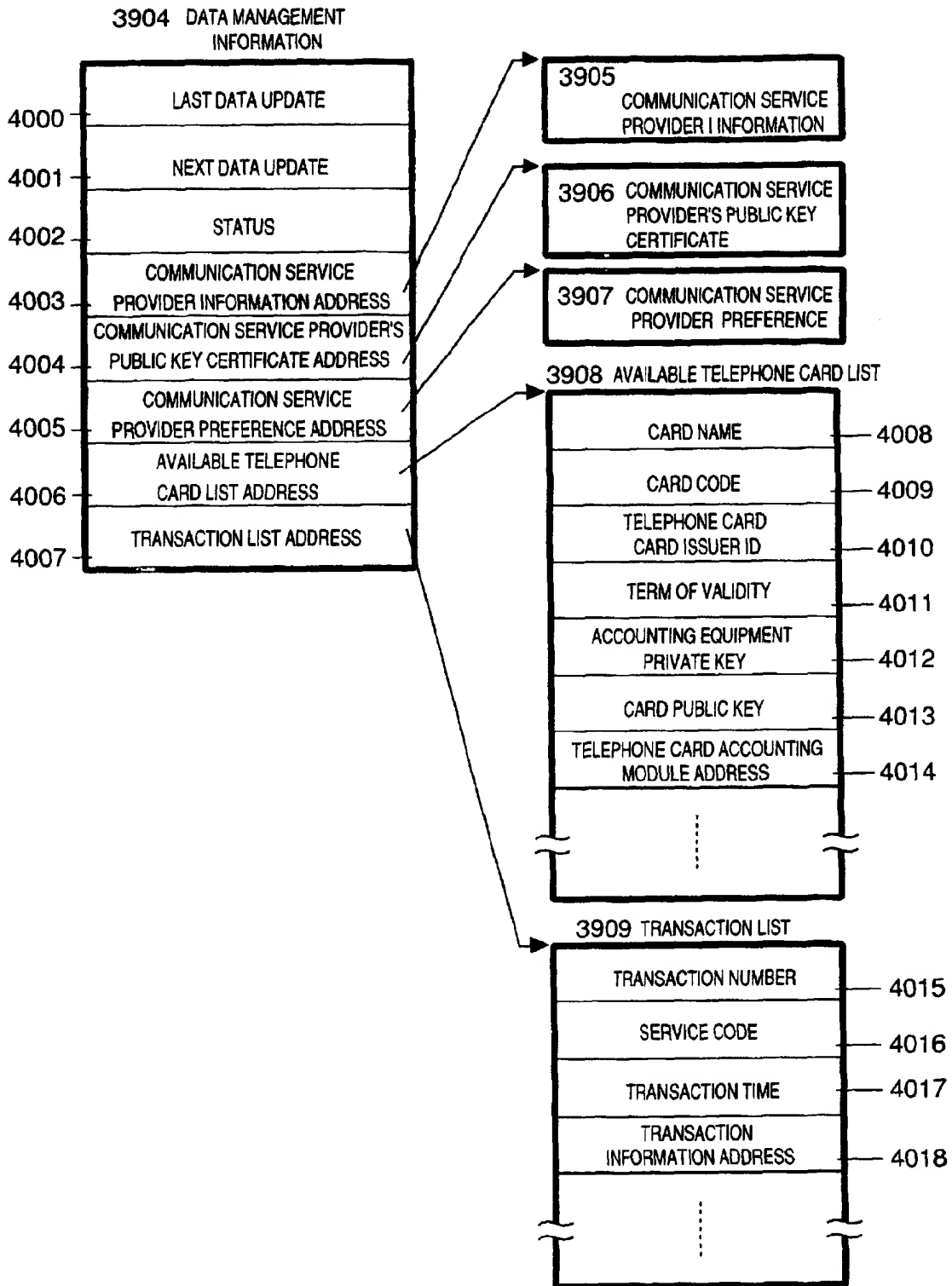


FIG. 41A

FIG. 41B

